Modicon M168 Controllers Network Connectivity Modules

User Guide

12/2012

S1A3839300.02

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information that is contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

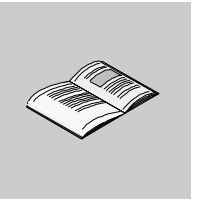
When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

© 2012 Schneider Electric. All rights reserved.

Table of Contents

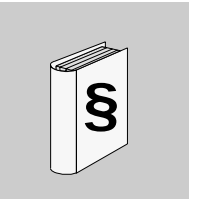


	Safety Information	**7**
	About the Book	**9**
Chapter 1	**Introduction**	**13**
	Overview	14
	Physical Description	15
	BACnet MS/TP Network Connectivity Module (TM168BACS)	17
	BACnet Ethernet Network Connectivity Module (TM168BACW)	19
	Modbus TCP Network Connectivity Module (TM168MODW)	22
Chapter 2	**Supported Functionality**	**25**
2.1	BACnet Functionality	26
	Supported BACnet Interoperability Building Blocks	27
	Supported BACnet Protocol Implementation Conformance Statements	29
	Supported BACnet Reporting	36
2.2	Modbus TCP Functionality	42
	Supported Modbus TCP Functionality	42
Chapter 3	**Installation**	**45**
	Installing or Removing a Module	45
Chapter 4	**Network Wiring and Topologies**	**49**
4.1	Supported Networks	50
	Supported BACnet Communication Networks	50
4.2	Wiring of the BACnet MS/TP Communication Network	53
	Cable Requirements for BACnet MS/TP Networks	54
	BACnet Standard 9.2	55
	Shielding	57
	BACnet MS/TP Network Configurations	59
4.3	Wiring of the Ethernet Communication Network	60
	Port Characteristics and Wiring	61
	Ethernet Network Connection	63
Chapter 5	**Commissioning**	**67**
5.1	Commissioning Communications	68
	Select the Controller and Configure the TM168BACS Module	69
	Select the Controller and Configure the TM168BACW Module	74
	Select the Controller and Configure the TM168MODW Module	78

5.2 Exporting Variables from SoHVAC 84
Exporting Variables From SoHVAC to a Modbus TCP Module 85
Exporting Variables from SoHVAC to a BACnet Module 87
Chapter 6 Using the Embedded Web Pages 91
6.1 Connecting to the Module for the First Time 92
Connecting to the Module 92
6.2 The Embedded Web Pages 96
Introducing the Web Browser 97
Accessing the Embedded Web Pages 99
Navigating the Embedded Web Pages (TM168BACW) 101
Navigating the Embedded Web Pages (TM168MODW) 103
6.3 Configuring the Modicon M168 Ethernet Modules 104
HTTP Account Administration 105
IP Parameter Configuration 107
SNMP Agent Configuration 110
Reboot Page 112
BACnet Network Parameter Configuration (TM168BACW) 113
Ethernet Port Configuration (TM168MODW) 114
DNS Configuration (TM168MODW) 115
6.4 Monitoring and Diagnosing the Status of the Modicon M168 Ethernet Module 116
Global Ethernet TCP/IP Statistics 117
Ethernet Port Statistics 118
SNMP Statistics 119
Diagnostic Log 120
BACnet Statistics (TM168BACW) 121
BACnet Discovery (TM168BACW) 122
Diagnosing BACnet (TM168BACW) 123
Modbus TCP Port Statistics (TM168MODW) 124
Modbus TCP Port Connections Statistics (TM168MODW) 125
Monitoring (TM168MODW) 126
6.5 Customizing Modicon M168 Connectivity Module Web Pages 128
Accessing the Web Configuration File 129
Editing the Web Configuration File 132
Chapter 7 Application Example 139
7.1 BACnet Application Example 139
Exporting Entities and Generating a BACnet Profile 140
Editing the BACnet Profile 142
Appendices 145
Appendix A What is BACnet? 147
A.1 Introduction to BACnet 148
Introduction to BACnet 148

A.2 BACnet Terminology 149
What is a BACnet Network? 150
BACnet Devices and Device Profiles 151
BACnet Objects 153
BACnet Properties 155
BACnet Services 156
BIBBs 157
BACnet Broadcasts 158
BACnet Command Priority 159
BACnet PICS 161
A.3 BACnet Routers, Gateways, BBMDs, and Foreign Devices 162
BACnet Routers and Gateways 163
BBMDs and Foreign Devices 164
Appendix B BACnet Troubleshooting and Diagnostics 165
B.1 General Troubleshooting 166
Troubleshooting Tasks 166
B.2 Diagnostics 167
No Communications with a New BACnet MS/TP Device 168
No Communications with a New BACnet/IP Device 170
Slow or Intermittent Communications with a BACnet MS/TP Segment . . 171
Communication Timeout 172
Slow Segments 173
BACnet Cannot Discover All Devices 174
Workstation Does Not Receive BACnet Alarm Signals 175
Undiscovered BACnet Device Objects 176
Unreadable Object Properties 177
Multiple BACnet Client Tools on PC 178
Appendix C Firmware Upgrade Procedures 179
C.1 Upgrading the TM168BACS 180
Downloading Firmware to a TM168BACS With BACbeat 180
C.2 Upgrading the TM168BACW and TM168MODW Modules 184
Downloading and Installing Unity Loader 185
Update the TM168BACW or TM168MODW Firmware with Unity Loader 186
C.3 Upgrading the TM168MODW Firmware 192
Update Firmware with Windows Explorer FTP 192
Appendix D SoHVAC Data Types 195
BACnet Objects 196
Modbus Objects 197
Glossary 199
Index 207

Safety Information



Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

NOTICE

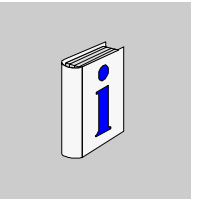
NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book



At a Glance

Document Scope

This document describes the network connectivity modules for Modicon M168 controllers. These controllers connect Modicon M168 modules to Modbus serial line networks.

You can use plug-in connectivity modules with Modicon M168 controllers that support BMS. Choose one of these modules for your network type:

Model Number	Network Connectivity
TM168BACS	BACnet MS/TP
TM168BACW	BACnet/IP
TM168MODW	Modbus TCP

Validity Note

These products work with SoHVAC version 2.0 or greater.

Firmware upgrades:

- TM168BACS *(see page 180)*: Upgrade the firmware over BACnet. Use any tool that is capable of writing to the file object and executing the BACnet command **ReinitializeDevice**.
- TM168BACW *(see page 180)*: Upgrade the firmware with the latest version of Unity Loader or use Windows Explorer to download the latest firmware.
- TM168MODW *(see page 192)*: Access the firmware for your module with Explorer's FTP command and overwrite it with new firmware from Schneider Electric.

NOTE: The BACnet examples used in this document are done using the BACbeat tool, which can be purchased from PolarSoft (www.polarsoft.biz/index.html).

Related Documents

Title of Documentation	Reference Number
Modicon M168 Air Handling Unit User Manual	TM168 UMAHU101
Modicon M168 Single and Twin Circuit Scroll Compressors Chiller User Manual	TM168 UMCHL1
SoHVAC Software User Manual	EIO0000000537.00
M168 Hardware Guide	EIO0000000533.00
Transparent Factory Network Design and Cabling Guide	35002987 (English), 35002988 (French), 35002989 (German), 35002990 (Spanish)

You can download these technical publications and other technical information from our website at www.schneider-electric.com.

Product Related Information

Only the user or integrator can be aware of all the conditions and factors present during installation and setup, operation, and maintenance of the application. Therefore, only that person can determine the automation and associated equipment and the related safeties and interlocks which can be effectively and properly used. When selecting automation and control equipment, and any other related equipment or software, for a particular application, the user or integrator must also consider any applicable local, regional, or national standards and/or regulations.

⚠ WARNING

REGULATORY INCOMPATIBILITY

Be sure that all equipment applied, and systems designed, comply with all local, regional, and national regulations and standards.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING

LOSS OF CONTROL

The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop, power outage, and restart.

Separate or redundant control paths must be provided for critical control functions. System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.

Observe all accident prevention regulations and local safety guidelines.[1]

Each implementation of this equipment must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

Start-up and Test

Before using electrical control and automation equipment after design and installation, the application and associated functional safety system must be subjected to a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such testing be made and that enough time is allowed to perform complete and satisfactory testing.

⚠ CAUTION

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in injury or equipment damage.

Verify that the completed system, including the functional safety system, is free from all short circuits and grounds, except those grounds installed according to local regulations. If high-potential voltage testing is necessary, follow recommendations in equipment documentation to help prevent injury or equipment damage.

Operation and Adjustments

Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly installed and operated.

It is sometimes possible to adjust the equipment incorrectly and thus produce unsatisfactory or unsafe operation. Always use the manufacturer instructions as a guide to functional adjustments. Personnel who have access to these adjustments must be familiar with the equipment manufacturer instructions and the machinery used with the electrical equipment.

Only those operational adjustments that are required by the machine operator should be accessible to the operator. Access to other controls should be restricted to help prevent unauthorized changes in operating characteristics.

User Comments

We welcome your comments about this document. You can reach us by e-mail at techcomm@schneider-electric.com.

Introduction

1

Overview

This chapter introduces the network connectivity modules for Modicon M168 controllers.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Overview	14
Physical Description	15
BACnet MS/TP Network Connectivity Module (TM168BACS)	17
BACnet Ethernet Network Connectivity Module (TM168BACW)	19
Modbus TCP Network Connectivity Module (TM168MODW)	22

Overview

Introduction

The network connectivity modules are a series of interchangeable fieldbus modules of a standardized form to fit the Modicon M168 line of controllers.

Key Features

The network connectivity modules offer these key features:

- Based on the module you choose, you have connectivity to BACnet MS/TP, BACnet/IP, or Modbus TCP networks.
- The modules are interchangeable with other network connectivity modules.
- The modules support all controllers in the Modicon M168 family that are enabled for BMS.
- The modules allow you to daisy chain the Modicon M168 controller on the network.
- The same SoHVAC software supports all Modicon M168 controllers and all Modicon M168 connectivity modules.

The SoHVAC programming software connects to the controller via a specialized serial port—the Programming Port—on the controller.

The BACnet Protocol

BACnet is a communication protocol developed by the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE) that allows products made by different manufacturers to be integrated into a single building automation control system. This protocol allows multiple BACnet devices to network together.

NOTE: Appendix A *(see page 147)* contains detailed information on BACnet.

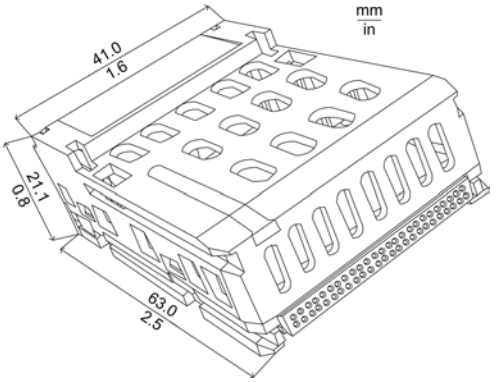
The Modbus Protocol

Modicon developed the Modbus protocol in 1978. It has been used by the industry as serial de facto standard since 1979. It is an application layer messaging protocol for client/server communication between devices that are connected on different types of buses or networks.

Physical Description

Description

All Modicon M168 network connectivity modules share the same form factor.



Controller Connector

Each network connectivity module includes a 50 pin connector, which plugs into the compatible Modicon M168 controller. The network connectivity module receives power from the controller via this 50 pin connector.

Operating Conditions

temperature	-20 °C...+65 °C (-4 °F...+149 °F)
	surrounding air temperature (max.): 70 °C (158 °F)
humidity	5%...95% without condensing and streaming (meets IEC 60068-2-3)
micro-environment	overvoltage category I
	pollution degree 2
altitude	0 m...2000 m (0 ft...6562 ft)
vibration	1.5 mm (0.58 inches) peak to peak from 3 Hz...13 Hz
	1 mm (0.3937 inches) peak to peak from 13 Hz...23 Hz
	2 g from 13 Hz ...150 Hz

Storage Conditions

temperature	-40 °C...+85 °C (-40 °F ... +185 °F)
humidity	5%...95% without condensing and streaming (meets IEC 60068-2-3)
free fall (in packaging)	1.2 m (4.265 ft) on 6 faces
shock	15 gn during 1 ms (meets IEC 60068-2-27)

Agency Approvals

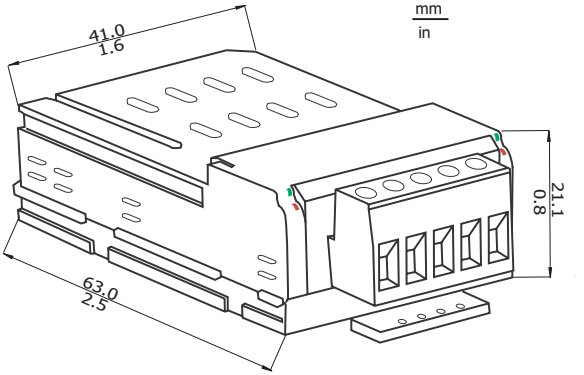
The following approvals for the network connectivity modules are marked on the module case of a network connectivity module:

- CE
- UL508 (with UR marking)

BACnet MS/TP Network Connectivity Module (TM168BACS)

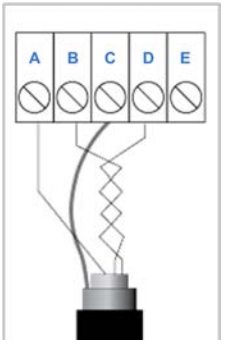
Description

The TM168BACS network connectivity module supports a BACnet MS/TP communication with a 5-position screw-type terminal block.



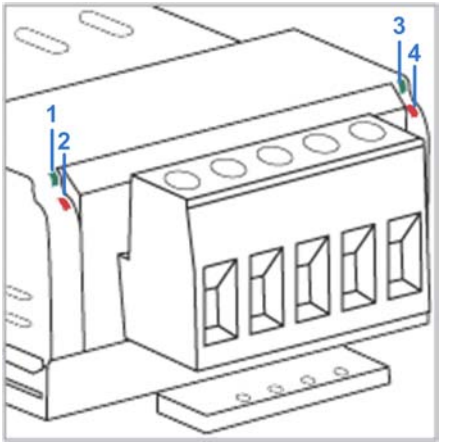
5-Pin Terminal Block

This table contains the wire connections for the 5-pin terminal block:

5-pin terminal block	BACnet MS/TP Pin Position	Signal
	A	signal common
	B	data-
	C	shield
	D	data+
	E	(not connected)
	NOTE: The letters identifying the connector pins are included for illustrative purposes only, and do not appear on the device.	
	terminal tightening torque (max.): 5-7 lb-in.	

LEDs

The module has 4 communication LEDs:



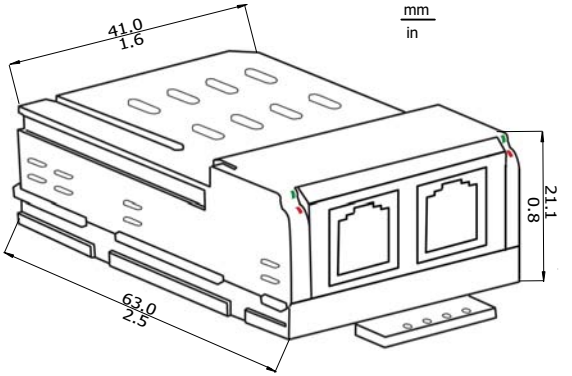
Position	Name	LED State	Description	Module State
1	MS	flashing green	Iso-phase is on and off at approximately 2.5 Hz (200 ms on, 200 ms off).	OK
		solid red	on	An event (like a host communication loss) has been detected.
		rapid flashing red at about 10 Hz	Iso-phase is on and off at approximately 10 Hz (50 ms on, 50 ms off).	The firmware is being downloaded to the module.
		flashing red/green alternating at about 1 Hz	Iso-phase is on and off at approximately 2.5 Hz (200 ms on, 200 ms off).	The firmware is being upgraded in Flash.
		single red flash	An invalid BACnet setting (such as a node address) is detected.	There is no communication on BACnet.
		double red flash	An invalid host profile.bin is detected.	BACnet communications are occurring only to provide the Device Object.
		triple red flash	A profile.bin is not detected for the host or module.	
2	Tx	flashing green	Iso-phase is on and off at approximately 2.5 Hz (200 ms on, 200 ms off).	Frames are being transmitted.
3	not labeled	solid red together with MS	on	An unrecoverable condition is detected.
4	Rx	flashing green	Iso-phase is on and off at approximately 2.5 Hz (200 ms on, 200 ms off).	Frames are being received.

NOTE: The numbers identifying the LEDs are included for illustrative purposes only, and do not appear on the device.

BACnet Ethernet Network Connectivity Module (TM168BACW)

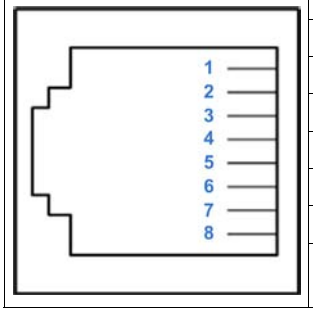
Description

The TM168BACW network connectivity module supports BACnet communications over Ethernet. The module has 2 Ethernet RJ45 ports:



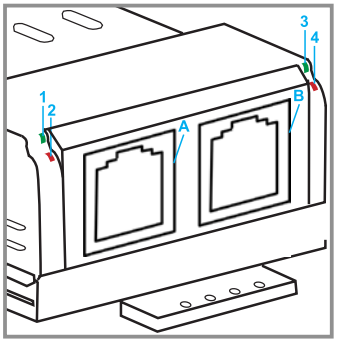
2-Port RJ45 Connector

Each Ethernet communication port uses the standard pinout:

Front View	Pin Number	Signal	Pair	Description
	1	TD+	A	Transmit +
	2	TD–	A	Transmit –
	3	RD+	B	Receive +
	4	Do not connect.	—	—
	5	Do not connect.	—	—
	6	RD–	B	Receive –
	7	Do not connect.	—	—
	8	Do not connect.	—	—

LEDs

Each device presents these LEDs:



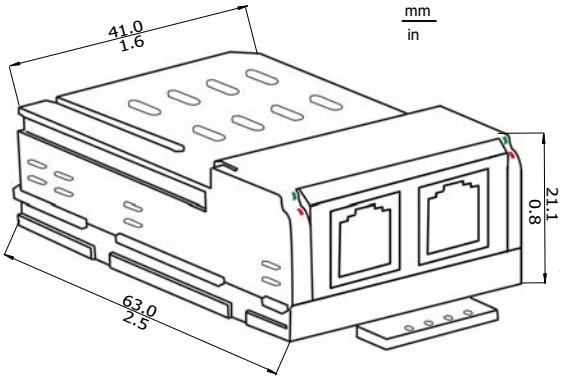
LED	Name	LED State	Description	Module State
1	MS (module status)	solid green	—	OK
		solid red	—	The module has detected an event (such as a host communications loss).
		single red flash	An invalid setting in the BACnet configuration is detected. Check the BACnet configuration.	BACnet communications are lost.
		double red flash	An invalid host profile is detected. Build the BACnet binary profile and compile and download the SoHVAC application.	BACnet communications provide only Device Object data.
		triple red flash	The host profile is missing in the module or host. Build the BACnet binary profile and compile and download the SoHVAC application.	BACnet communications provide only Device Object data.
2	Link/Activity Port 1	solid green	An Ethernet link is present at 100 Mbps.	The module has detected an Ethernet link.
		flashing green	An Ethernet link is present with Ethernet traffic at 100 Mbps.	The module detects Ethernet traffic.
		solid yellow	An Ethernet link is present at 10 Mbps.	The module detected an Ethernet link.
		flashing yellow	An Ethernet link is present with Ethernet traffic at 10 Mbps.	The module detects Ethernet traffic.

LED	Name	LED State	Description	Module State
3	NS (network status)	flashing green	The network operates normally.	OK
		4 flashes	A duplicate IP condition exists.	The module operates offline.
		5 flashes	The module attempts to get an IP configuration from BootP server.	The module sends BOOTP/DHCP requests to a BootP server and awaits a reply.
		6 flashes	Operations are normal with default IP addressing settings.	The BootP request timed out. The module applies the default IP address (85.16.x.y).
		7 flashes	Operations are in kernel mode.	The module attempts to acquire a new firmware image.
4	Link/Activity Port 2	solid green	An Ethernet link is present at 100 Mbps.	The module detects an Ethernet link.
		flashing green	An Ethernet link is present with Ethernet traffic at 100 Mbps.	The module detects Ethernet traffic.
		solid yellow	An Ethernet link is present at 10 Mbps.	The module detects an Ethernet link.
		flashing yellow	An Ethernet link is present with Ethernet traffic at 10 Mbps.	The module detects Ethernet traffic.

Modbus TCP Network Connectivity Module (TM168MODW)

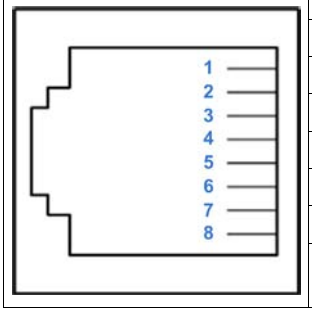
Description

The TM168MODW network connectivity module supports Modbus TCP communications over Ethernet. The module has 2 Ethernet RJ45 ports:



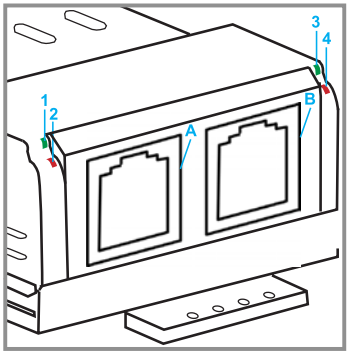
2-Port RJ45 Connector

Each Ethernet communication port uses the standard pinout:

Front View	Pin Number	Signal	Pair	Description
	1	TD+	A	Transmit +
	2	TD–	A	Transmit –
	3	RD+	B	Receive +
	4	Do not connect.	–	–
	5	Do not connect.	–	–
	6	RD–	B	Receive –
	7	Do not connect.	–	–
	8	Do not connect.	–	–

LEDs

Each device presents these LEDs:



LED descriptions:

LED	Name	LED State	Description	Module State
1	MS (module status)	green	on	OK
			off	There is no power and no power-up is in progress.
2	Link/Activity Port 1	solid green	An Ethernet link is present at 100 Mbps.	The module detects an Ethernet link.
		flashing green	An Ethernet link is present with Ethernet traffic at 100 Mbps.	The module detects Ethernet traffic.
		solid yellow	An Ethernet link is present at 10 Mbps.	The module detects an Ethernet link.
		flashing yellow	An Ethernet link is present with Ethernet traffic at 10 Mbps.	The module detects Ethernet traffic.
3	NS (network status)	solid green	The network is operating normally.	OK
		4 flashes	A duplicate IP condition exists.	The module operates offline.
		5 flashes	The module attempts to get an IP configuration from BootP server.	The module sends BOOTP/DHCP requests to a BootP server and awaits a reply.
		6 flashes	Operations are normal with default IP addressing settings.	The BootP request timed out. The module applies the default IP address (85.16.x.y).
		7 flashes	Operations are in kernel mode.	The module attempts to acquire a new firmware image.

LED	Name	LED State	Description	Module State
4	Link/Activity Port 2	solid green	Link is present at 100 Mbps.	Module has detected an Ethernet link.
		flashing green	Link is present with Ethernet traffic at 100 Mbps.	Module is detecting Ethernet traffic.
		solid yellow	Link is present at 10 Mbps.	Module has detected an Ethernet link.
		flashing yellow	Link is present with Ethernet traffic at 10 Mbps.	Module is detecting Ethernet traffic.

Supported Functionality

2

Overview

This chapter contains the supported services for the relevant protocol.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
2.1	BACnet Functionality	26
2.2	Modbus TCP Functionality	42

2.1 BACnet Functionality

Introduction

This section describes the supported services for the BACnet protocol.

What Is in This Section?

This section contains the following topics:

Topic	Page
Supported BACnet Interoperability Building Blocks	27
Supported BACnet Protocol Implementation Conformance Statements	29
Supported BACnet Reporting	36

Supported BACnet Interoperability Building Blocks

Introduction

The network connectivity module provides a set of BACnet interoperability building blocks (BIBBs) that support the communication services between a client (device A) and a server (device B). For example, device B may provide data to device A.

Building Block Categories

The supported BIBBs fall into 3 categories:

- *data sharing blocks*: These blocks share the values of BACnet objects and sometimes modify BACnet object values in other objects.
- *alarm and event blocks*: These blocks generate event notifications and provide alarm and event summaries.
- *device management blocks*: These blocks respond to status queries, requests for BACnet object information, and communication control messages.

These categories are described below.

Data Sharing Block Services

This table describes the supported BIBB services for data sharing blocks:

BIBB Name	BACnet Service	Type	Description
DS-RP-B	ReadProperty	Initiation	Device A returns a single value for each event that it reads.
DS-RPM-B	ReadPropertyMultiple	Initiation	Device A returns multiple values for each event that it reads.
DS-WP-B	WriteProperty	Initiation	Device B allows device A to change a single value at one time.
DS-WPM-B	WritePropertyMultiple	Initiation	Device B allows device A to change multiple values at one time.
DS-COV-B	SubscribeCOV	Execution	Device B supports at least 5 concurrent subscriptions. **NOTE:** Device B does not support indefinite lifetime subscriptions.
	ConfirmedCOVNotification	Initiation	
	UnconfirmedCOVNotification	Initiation	

Alarm and Event Block Services

This table describes the supported BIBB services for alarm and event blocks:

BIBB Name	BACnet Service	Type	Description
AE-ASUM-B	GetAlarmSummary	Execution	Device B provides a BACnet alarm and event summary.
AE-N-I-B	ConfirmedEventNotification	Initiation	Device B generates BACnet alarm and event notifications.
	UnconfirmedEventNotification	Initiation	
AE-ACK-B	AcknowledgeAlarm	Execution	Device B generates acknowledgments of previously transmitted BACnet alarm or event notifications.
AE-INFO-B	GetEventInformation	Execution	Device B provides BACnet alarm and event information to device A.

Device Management Block Services

This table describes the supported BIBB services for device management blocks:

BIBB Name	BACnet Service	Type	Description
DM-DDB-A	Who-Is	Initiation	Device A seeks information about the attributes of other devices and interprets device announcements (dynamic device binding).
	I-Am	Execution	
DM-DDB-B	Who-Is	Execution	Device B provides information about its attributes and responds to requests to identify itself (dynamic device binding).
	I-Am	Initiation	
DM-DOB-B	Who-Has	Execution	Device B device provides address information about its objects upon request (dynamic object binding).
	I-Have	Initiation	
DM-DCC-B	DeviceCommunicationControl	Execution	Device B responds to communication control exercised by device A.
DM-TS-B	TimeSynchronization	Execution	Device B interprets time synchronization messages from device A.
DM-RD-B	ReinitializeDevice	Execution	Device B is reinitialized. The initialization is based on requests from device A to support firmware downloads over BACnet with a WARMSTART or a COLDSTART. (See note.)

NOTE: WARMSTART and COLDSTART:

- WARMSTART (for DM-RD-B): Reboot the communication option module only. If the firmware and Boot codes are present in the communication module, the firmware is upgraded. The Modicon M168 controller does not reboot.
- COLDSTART (for DM-RD-B): Reboot the Modicon M168 controller and the communication module. Application parameters are reset to default values.

Supported BACnet Protocol Implementation Conformance Statements

Introduction

This topic provides you with the supported protocol implementation conformance statements (PICS) objects for a BACnet network.

NOTE: Except where noted, there is no fixed limit for the number of objects. Generally, the limit is determined by the memory consumption. Multi-state value (MV) objects use the most memory. When fewer MV objects are used, more memory is available for analog value (AV) or binary value (BV) objects. However, the maximum number of notification class objects is 6.

NOTE: Any property indicated as writable loses the modifications after a power cycle (except MAX_Master, Max_Info_Frames and Device_Instance).

This table shows the status and control objects for the Modicon M168 controller:

Description	Values
device (DV)	These strings and values define the device characteristics.
analog value (AV)	This is the present value.
binary value (BV)	This is the present value (active/inactive).
multi-state value (MV)	There is a maximum of 16 states.
notification class	This is the destination for BACnet alarm signals (6-object maximum).

Device (DV) Object

Device object properties with read/write access lose their modified values after a power cycle, except for MAX_Master and Max_Info_Frames.

Property	Access	Device Object Property Values (DV)
Object_Identifier	read/write	
Object_Name	read/write	This name is determined at startup from the profile.
Object_Type	read	DEVICE
System_Status	read	OPERATIONAL
	read	NON_OPERATIONAL (This value indicates a detected non-operational event, such as a loss of internal communications.)
Vendor_Name	read	Schneider Electric
Vendor_Identifier	read	10
Model_Name	read	This property indicates the model name of the network connectivity module in the Modicon M168 controller.
Firmware_Revision	read	This property indicates the firmware version of the network connectivity module.

Property	Access	Device Object Property Values (DV)
Application_Software_Version (of BMG software)	read	This property is defined in the profile. (The default value is taken from ProjectVersionProjectRevision in SoHVAC.)
Location	write	This property is defined in the profile. (The default value is in Model_Name.)
Description	write	This property is defined in the profile. (The default value is in Model_Name.)
Protocol_Version	read	BACnet Version 1
Protocol_Revision	read	BACnet Revision 4
Active_COV_Subscriptions	read	This variable reflects the current status of communications. **NOTE:** More than 10 COV subscriptions are supported. Owing to APDU size limitations from BACnet MS/TP, only 10 active subscriptions can be reported. If there are more than 10 active subscriptions, the response is “reject (other).”
Protocol_Services_Supported	read	`ReadProperty`
	read	`ReadPropertyMultiple`
	read	`WriteProperty`
	read	`WritePropertyMultiple`
	read	`Who-is`
	read	`I-Am`
	read	`Who-Has`
	read	`I-Have`
	read	`DeviceCommunicationControl`
	read	`ReinitializeDevice`
	read	`TimeSynchronization`
Protocol_Object_Types_Supported	read	Device
	read	Binary Value
	read	Analog Value
	read	Multi-State Value
Object_List (reflecting profile objects)	read	This object list is determined at startup from the profile.
Max_APDU_Length_Accepted	read	BACnet/IP: 1476
	read	BACnet MS/TP: 480
Segmentation_Supported	read	NO_SEGMENTATION
Local_Time	read	Hours:Minutes:Seconds
Local_Date	read	Day-Month-Year
APDU_Timeout	read	1 ... 255 ms (3 ms default)

Property	Access	Device Object Property Values (DV)
Number_Of_APDU_Retries	read	0 ... 5 (the maximum number of times an APDU can be retransmitted) **NOTE:** The default value is 3. This value cannot be edited from the LCD screen on the controller. The value is determined at startup from the profile.
Device_Address_Binding	read	empty list
Database_Revision	read	1 ... 65535
Profile_Name	read	This name is determined at startup from the profile.
MAX_Master	read/write	1 ... 127 (configured for Modicon M168 in SoHVAC)
Max_Info_Frames	read/write	1 ... 3 (configured for Modicon M168 in SoHVAC)

Analog Value (AV) Objects

Analog value object properties with read/write access lose their modified values after a power cycle.

Property	Access	Analog Value Object Values (AV)
Object_Identifier	read/write	
Object_Name	read/write	This entity name is used on SoHVAC.
Object_Type	read	Analog Value
Present_Value	read/write	This property is writable only when Out_Of_Service is True.
Description	read/write	name tag
Status_Flags	read	IN_ALARM, FAULT, OVERRIDDEN, OUT_OF_SERVICE (The default setting for each is false.)
Event_State	read	possible settings: NORMAL (default), FAULT
Reliability	read	possible settings: NO_FAULT_DETECTED (default), NO_SENSOR, OVER_RANGE, UNDER_RANGE, OPEN_LOOP, SHORTED_LOOP, UNRELIABLE_OTHER.
Out_Of_Service	read/write	true or false
Units	read	The default is NO_UNITS.
COV_Increment	read/write	The factory default value is 0. The present setting is the value most recently input by the SoHVAC tool.
Time_Delay	read/write	The factory default value is 0. The present setting is the value most recently input by the SoHVAC tool.
Notification_Class	read/write	The factory default value is 0. The present setting is the value most recently input by the SoHVAC tool.
High_Limit	read/write	The factory default value is 0. The present setting is the value most recently input by the SoHVAC tool.
Low_Limit	read/write	The factory default value is 0. The present setting is the value most recently input by the SoHVAC tool.

Property	Access	Analog Value Object Values (AV)
Deadband	read/write	The factory default value is 0. The present setting is the value most recently input by the SoHVAC tool.
Limit_Enable	read/write	possible values: LowLimitEnable and HighLimitEnable (The default setting is DISABLED.)
Event_Enable	read/write	These flags separately enable and disable reporting of TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is DISABLED.)
Acked_Transitions	read	These flags separately indicate the receipt of acknowledgments for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is cleared.)
Notify_Type	read/write	This type defines whether the notifications generated by the object should be BACnet event (default) or alarm signals.
Event_Time_Stamps	read	This is an array of BACnetTimeStamps of the last TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is cleared.)

Binary Value (BV) Objects

Binary value object properties with read/write access lose their modified values after a power cycle.

Property	Access	Binary Value Object Values
Object_Identifier	read/write	
Object_Name	read/write	This entity name is used in SoHVAC (16-character maximum).
Object_Type	read	Binary Value
Present_Value	read/write	This property is writeable when Out_Of_Service isTrue.
Description	read/write	The name tag is from SoHVAC (16-character maximum).
Status_Flags	read	IN_ALARM, FAULT, OVERRIDDEN, OUT_OF_SERVICE (The default setting for each is False.)
Event_State	read	This property is always set to Normal.
Reliability	read	possible settings: NO_FAULT_DETECTED (default), NO_SENSOR, OPEN_LOOP, SHORTED_LOOP, UNRELIABLE_OTHER.
Out_Of_Service	read/write	True/False
Inactive_Text	read/write	The default value is from the profile.
Active_Text	read/write	The default value is from the profile.
Time_Delay	read/write	
Notification_Class	read/write	The factory default value is 0. The current value is the last one entered by the SoHVAC tool.
Alarm_Value	read/write	Present_Value has this value specified by this type when it generates a TO-OFFNORMAL event.
Event_Enable	read/write	possible settings: NORMAL (default), FAULT

Property	Access	Binary Value Object Values
Acked_Transitions	read	These flags indicate the receipt of acknowledgments for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is cleared.)
Notify_Type	read/write	The factory default value is 0. The current value is the last one entered by the SoHVAC tool.
Event_Time_Stamps	read	This is an array of BACnetTimeStamps of the last TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is cleared.)

Multi-State Value (MV) Objects

This table shows the Multi-State Value (MV) objects and their values:

Property	Access	Multi-State Value Object Values
Object_Identifier	read/write	
Object_Name	read/write	This is the name tag from SoHVAC (16-character maximum).
Object_Type	read	Multi-State Value
Present_Value	read/write	This property is configured by SoHVAC (16 maximum states). **NOTE:** Present_Value is writeable only when Out_Of_Service is True.
Description	read/write	This is the name tag from SoHVAC (16-character maximum).
Device_Type	read	Multi_State_Value
Status_Flags	read	IN_ALARM, FAULT, OVERRIDDEN, OUT_OF_SERVICE (The default for each is False.)
Event_State	read	possible settings: NORMAL (default), FAULT
Reliability	read	possible settings: NO_FAULT_DETECTED (default), NO_SENSOR, OVER_RANGE, UNDER_RANGE, OPEN_LOOP, SHORTED_LOOP, UNRELIABLE_OTHER.
Out_Of_Service	read/write	true or false
Number_Of_States	read	The number of states is configured in SoHVAC (16-state maximum).
State_Text	read/write	This property is configured in SoHVAC (16-character maximum).
Time_Delay	read	The factory default value is 0. The current value is the last one entered by the SoHVAC tool.
Notification_Class	read/write	The factory default value is 0. The current value is the last one entered by the SoHVAC tool.
Alarm_Values	read/write	This list of values specifies the state that Present_Value equals before the generation of a TO-OFFNORMAL event.
Fault_Values	read/write	This list of values specifies the state that Present_Value equals before the generation of a TO-FAULT event.
Event_Enable	read/write	These flags separately enable and disable reporting of TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is DISABLED.)

Property	Access	Multi-State Value Object Values
Acked_Transitions	read/write	These flags separately indicate the receipt of acknowledgments for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is cleared.)
Notify_Type	read/write	Defines whether the notifications generated by the object should be BACnet event (default) or alarm signals.
Event_Time_Stamps	read	This is an array of BACnetTimeStamps of the last TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. (The default setting is cleared.)

Notification Objects

This table shows the notification objects and their access properties:

Property	Access	Notification Object Values
Ack_Required	read/write	This property has 3 separate flags to indicate that acknowledgment is required in notifications generated for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL event transitions. The type is `BACnetEventTransitionBits`.
Description	read/write	A string of printable characters whose content is not restricted. The type is `CharacterString`.
Notification_Class	read	This numeric value indicates the notification class. It is equal to the instance number of the Notification Class object. Objects that initiate events use this number to refer to this Notification Class object indirectly. The type is `Unsigned`.
Object_Identifier	read	This numeric code identifies the object. It is unique within the BACnet device that maintains it. The type is `BACnetObjectIdentifier`.
Object_Name	read/write	The string represents a name for the object that is unique within the BACnet device that maintains it (1-character minimum). The set of characters used in the Object_Name is restricted to printable characters. The type is `CharacterString`.
Object_Type	read	This property indicates membership in a particular object type class. The value of this property is NOTIFICATION_CLASS. The type is `BACnetObjectType`.
Priority	read/write	This property conveys the priority used for event notifications for TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events. The priority range is 0...255 (inclusive). A lower number indicates a higher priority. The type is `BACnetARRAY`[3] of `Unsigned`.

<table>
<tr><th>Property</th><th>Access</th><th colspan="3">Notification Object Values</th></tr>
<tr><td rowspan="8">Recipient_List</td><td rowspan="8">read/write</td><td colspan="3">This property provides a list of one or more destinations to which notifications are sent when event-initiating objects using this class detect an event (type = List of BACnetDestination). The destinations themselves define a structure of parameters:</td></tr>
<tr><td>Parameter</td><td>Type</td><td>Description</td></tr>
<tr><td>Valid Days</td><td>BACnetDaysOfWeek</td><td>The set of days of the week on which this destination may be used between From Time and To Time.</td></tr>
<tr><td>From Time / To Time</td><td>Time</td><td>The window of time (inclusive) during which the destination is viable on the days of the week Valid Days.</td></tr>
<tr><td>Recipient</td><td>BACnetRecipient</td><td>The destination device(s) to receive notifications.</td></tr>
<tr><td>Process Identifier</td><td>Unsigned32</td><td>The unique identifier of a process within the recipient device that is to receive the event notification.</td></tr>
<tr><td>Issue Confirmed Notifications</td><td>Boolean</td><td>TRUE: Confirmed notifications are sent.
FALSE: Unconfirmed notifications are sent.</td></tr>
<tr><td>Transitions</td><td>BACnet Event Transition Bits</td><td>This set of 3 flags indicates the transitions (TO-OFFNORMAL, TO-FAULT, TO-NORMAL) for which this recipient is suitable.</td></tr>
</table>

Supported BACnet Reporting

Description

Intrinsic reporting is a feature of BACnet devices that presents one or more BACnet alarm or BACnet event sources that are intrinsic to the device. These intrinsic sources generate notifications that can be directed to one or more clients.

Certain BACnet objects can support intrinsic reporting by providing optional properties for defining the type of BACnet alarm or BACnet event to be generated and options for handling and routing of the notifications. Internal status changes and events can also use intrinsic reporting to generate diagnostic notifications.

If an object provides intrinsic reporting, changes of value of specific properties of the object, or changes of status internal to the object, trigger event notifications that are sent to one or more destinations based on notification class. Typically, event notifications are sent to operators or logging devices represented by processes within a notification-client device.

Intrinsic reporting by BACnet devices is more fully described in section 13.2 of the ANSI/ASHRAE Standard 135-2004.

These objects support intrinsic reporting of alarms and events:

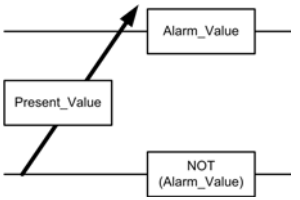
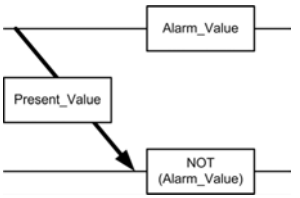
- Binary Value
- Analog Value
- Multi-State Value

Binary Value

Intrinsic reporting for the binary value object uses the Alarm_Value property to define the OFF_NORMAL value for the Present_Value of the binary value. These properties are used in intrinsic reporting:

Property	Description
Alarm_Value	The Alarm_Value property defines which state (active or inactive) generates a TO-OFFNORMAL event.
Time_Delay	The Time_Delay property is the minimum range (in seconds) that the Present_Value occupies during the generation of an event (such as a TO-OFFNORMAL event or a TO-NORMAL event).
Event_Enable	The Event_Enable property contains the TO-OFFNORMAL, TO-NORMAL, and to-fault flags that indicate the events that are generated.

These are visual representations of intrinsic reporting:

Diagram
TO-OFFNORMAL event when the Present_Value transitions to a configured Alarm_Value: 
TO-NORMAL event when the Present_Value transitions from Alarm_Value to NOT (Alarm_Value): 

Analog Value

The properties in this table are used in intrinsic reporting:

Property	Description
Low_Limit	The Low_Limit is used to generate the TO-OFFNORMAL event if the Present_Value falls below this limit for the Time_Delay duration, the Limit_Enable property has the lowLimitEnable flag set, and the TO-OFFNORMAL flag is set in the Event_Enable property.
High_Limit	The High_Limit generates the TO-OFFNORMAL event under these conditions: ● The TO-OFFNORMAL event if the Present_Value goes above this limit for the Time_Delay duration. ● The highLimitEnable flag of the Limit_Enable property is set. ● The TO-OFFNORMAL flag is set in the Event_Enable property.
Deadband	The deadband property is used to avoid a burst of events when the Present_Value is passing through the Low_Limit or High_Limit values. The present value is below the High_Limit – Deadband or Low_Limit + Deadband for the Time_Delay duration when it returns to the NORMAL state (TO-NORMAL event), .
Limit_Enable	The Limit_Enable property contains the lowLimitEnable and highLimitEnable flags to enable or disable checking of high and low limits on the Present_Value.
Event_Enable	The Event_Enable property contains the TO-OFFNORMAL, TO-NORMAL, and TO-FAULT flags to select which events are generated.
Time_Delay	The Time_Delay property is the minimum range (in seconds) that the Present Value occupies during the generation of an event such as TO-OFFNORMAL or TO-NORMAL.

These are visual representations of intrinsic reporting for a TO-OFFNORMAL event:

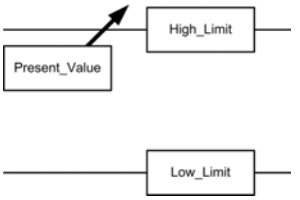
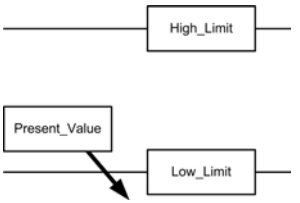
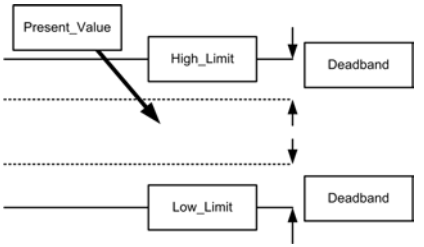
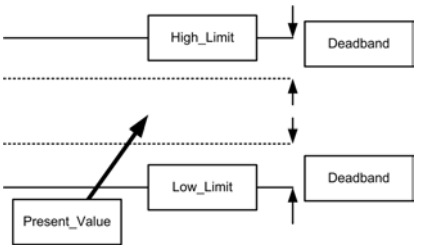
Diagram
TO-OFFNORMAL event when the Present_Value of the AV object goes above the High_Limit: 

Diagram
TO-OFFNORMAL event when the Present_Value of the AV object goes below the Low_Limit: 

A TO-NORMAL event is generated by the Analog object when the Present_Value passes from beyond the High_Limit or Low_Limit to the range between the deadband. These are visual representations of intrinsic reporting for such a TO-NORMAL event:

Diagram
TO-NORMAL event when the Present_Value of the Analog Value Object passes below the High_Limit – Deadband: 
TO-NORMAL event when the Present_Value of the Analog Value Object passes above the Low_Limit + Deadband: 

Multi-State Value

Configure the states that generate a BACnet alarm signal (Alarm_Values) and also the states that generate notification for a detected BACnet fault (Fault_Values) in order to permit intrinsic reporting for the Multi-State Value object. These properties are used in intrinsic reporting:

Property	Description
Time_Delay	The Time_Delay property is the minimum range (in seconds) that the Present Value occupies during the generation of an event such as TO-OFFNORMAL or TO-NORMAL.
Alarm_Values	The Alarm_Values property is an array of multi-state values that will generate TO-OFFNORMAL event.
Fault_Values	The Fault_Values property is an array of multi-state values that generates a TO-FAULT event.
Event_Enable	The Event_Enable property contains the TO-OFFNORMAL, TO-NORMAL, and TO-FAULT flags to select which events are generated.
Notify_Type	The Notify_Type property shall indicate whether notifications for this object shall be events or alarms.
Event_Time_Stamps	The Event_Time_Stamps property is an array of the BACnetTimeStamp of the last TO-OFFNORMAL, TO-FAULT, and TO-NORMAL events.

These are visual representations of intrinsic reporting for a TO-OFFNORMAL and a TO-FAULT event:

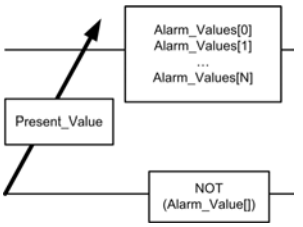
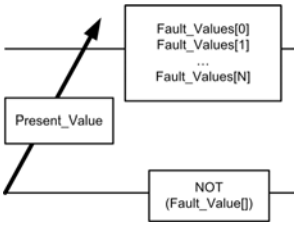
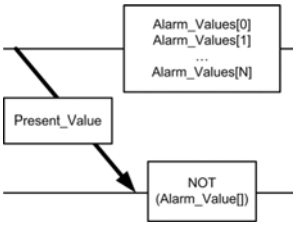
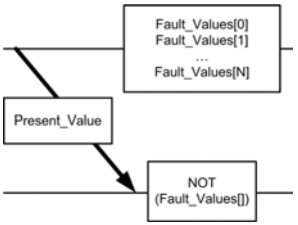
Diagram
TO-OFFNORMAL event when the Present_Value of the Multi-State Value object transitions to one of the states listed as a BACnet alarm (Time_Delay): 

Diagram
TO-FAULT event when the Present_Value of the Multi-State Value object transitions to one of the states listed as a BACnet fault state (Time_Delay): 

These are visual representations of intrinsic reporting for a TO-NORMAL event:

Diagram
TO-NORMAL event for Multi-State Value – removal of BACnet alarm conditions: 
TO-NORMAL event for Multi-State Value – removal of BACnet fault conditions: 

2.2 Modbus TCP Functionality

Supported Modbus TCP Functionality

Introduction

The TM168MODW module provides Modbus TCP connectivity for your Modicon M168 controller. Modbus TCP provides very flexible connectivity to a wide range of products for your Modicon M168 controller.

Connections

With the TM168MODW module, you can connect a Modicon M168 controller to any system with Modbus TCP clients, including these:

- PLC (function blocks or IO scanner)
- HMI
- SCADA
- mobile application
- Building Management System (BMS)

Use these Unit IDs:

Unit ID	Description
255	Access the TM168 controller (for 43/14 and 8/22 only).
14	Access the Modicon M168 controller.

Refer to the Modbus home page (www.modbus.org) for technical information about the Modbus protocol and Modbus TCP.

Supported Modbus Functions (Local to TM168MODW)

The TM168MODW module answers some Modbus requests locally (using Unit ID 255) through these Modbus commands:

Function Code		Subcode		Name of Function Code	Description
Hex	Dec	Hex	Dec		
08	08	16	22	Ethernet diagnostics (dual-port)	This code provides Ethernet statistics and diagnostics for dual-port devices.
2B	43	0E	14	read device identification	The Read Device ID (basic) returns the reference number and firmware revision level of the device.

Supported Modbus Functions (Controller)

If the Unit ID of the Modbus TCP message is 1...255, the Modbus request is forwarded to the controller.

The SoHVAC Software Manual (EIO0000000537.00) is in the documentation folder of your SoHVAC install folder. You can also downloaded it from www.schneider-electric.com. It contains these items:

- A list of Modbus Commands supported by the controller
- Updated information regarding supported function codes.

Only these variable types can be exported:

Entity	SoHVAC Data Type
Analog In	CJ_ANALOG (only the value)
Analog Out	CJ_WORD
Clock	CJ_DATETIME
Timer	CJ_WORD
Par	all
Pers	all
Var	all
Fixs	all

NOTE: The 32-bit data types (CJ_LONG, CJ_DWORD, CJ_DATETIME, CJ_DATE, and CJ_TIME) take up 2 rows in the Register Vars list. The low 16 bits are in the first row and the high 16 bits are in the second one.

Modbus clients receive these Modbus function codes from the master to access the Register Vars Table:

Function Code	Description
03	Read multiple holding registers.
04	Read input registers.
06	Write single holding register.
16	Write multiple registers.
23	Read/write multiple register (10-register maximum).

Machine builders can use the Modbus documentation exported in HTML format from the SoHVAC software to have a list of variables that are exported on Modbus TCP and their Modbus addresses and formats. Refer to the discussion about exporting SoHVAC variables *(see page 85)*.

NOTE: SoHVAC addresses use the 4x format (starting at 1). For Modbus clients that use the %MW format (starting at 0), the Modbus HTML documentation gives both addresses.

System integrators and machine installers should consult the machine manual for the available application variables on Modbus.

Number of Modbus Connections

The Modbus TCP communication module supports 8 simultaneous Modbus TCP connections.

If a Modbus client requests to open a connection when all 8 connections are being used, the TM168MODW module closes the connection that has the oldest last transaction.

Installation

3

Installing or Removing a Module

Before you begin

Use these directions to mount the network connectivity module and connect the cables.

Before you attempt to install or remove a module from the Modicon M168 controller, read the following information.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Read and understand this manual and the manuals of the controller before installing this module.
- Installation must be performed by qualified personnel.
- Users are responsible for compliance with all international and national electrical code requirements with respect to grounding of all equipment.
- Do not touch unshielded components or terminal screw connections with voltage present.
- Perform these steps before you install the module in the controller or remove it from the controller:
  - Disconnect all power.
  - Place a “Do not turn on” label on all power disconnects.
  - Lock all power disconnects in the open position.

Failure to follow these instructions will result in death or serious injury.

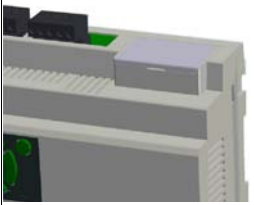
Electrostatic discharge (ESD) can cause immediate or delayed damage to the module or the controller whenever you handle components.

NOTICE
ELECTROSTATIC DISCHARGE • Use measures in accordance with IEC 61340-5-2 when handling the module or the controller. • Do not touch any internal components. **Failure to follow these instructions can result in equipment damage.**

Verify that the order number on the nameplate of the module corresponds to the module that you want to install.

Plugging a Module into the Controller Slot

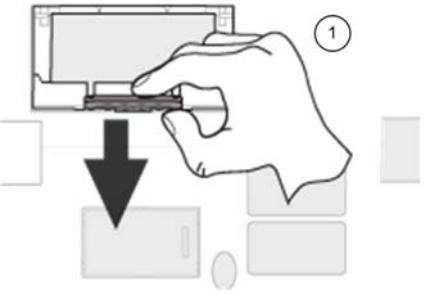
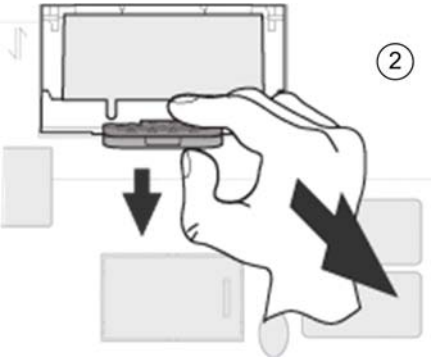
Mount your module in the Modicon M168 controller.

Step	Action
1	Remove the plastic cover from the network connectivity slot, shown in the top right: 
2	Slide the module into the top right slot of the Modicon M168 controller: **NOTE:** The module lever clicks when the module is properly seated in the controller.
3	Make these connections: • For BACnet MS/TP networks, attach the included mating connector to the module. • For BACnet/IP or Modbus TCP networks, no mating connector is needed. Use a regular Ethernet cable that is terminated with an RJ45 connector.
4	Apply power to the Modicon M168 controller.

NOTE: After the module is mounted, connect the cables. When this is done, commission the modules *(see page 67)* to complete the installation process.

Removing a Module

Remove a module from the Modicon M168 controller.

Step	Action
1	Push the snap lock handle on the module back 
2	While holding the snap lock handle back, pull the module out of the controller slot. 

Network Wiring and Topologies

4

Overview

This chapter describes network wiring and provides examples of how to connect to such networks.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
4.1	Supported Networks	50
4.2	Wiring of the BACnet MS/TP Communication Network	53
4.3	Wiring of the Ethernet Communication Network	60

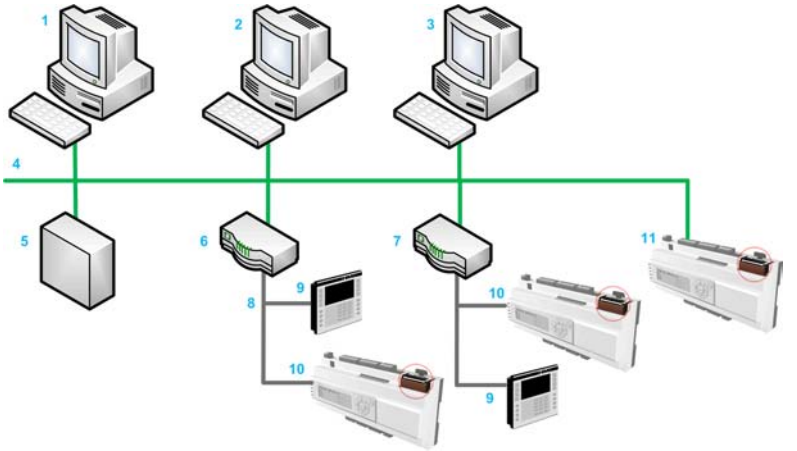
4.1 Supported Networks

Supported BACnet Communication Networks

Description

The Modicon M168 controller provides BACnet communication capability, which allows it to be integrated into a BACnet system via:

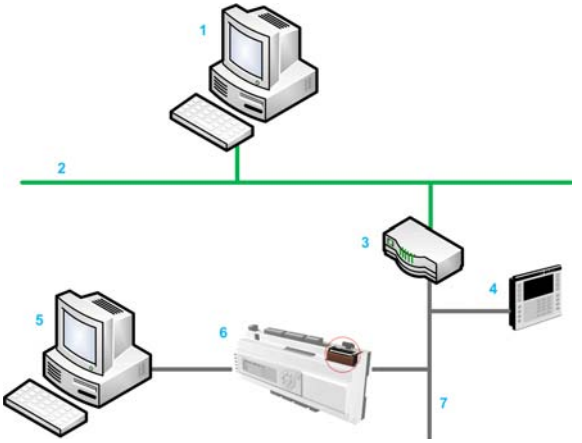
- RS-485 (BACnet MS/TP)
- Ethernet (BACnet/IP)



1 BACnet operator workstation (B-OWS), vendor A (for example, the Continuum CyberStation from Schneider Electric)
2 B-OWS, vendor B
3 B-OWS, vendor C
4 BACnet/IP network
5 BACnet Lighting, vendor A
6 BACnet router between BACnet/IP and BACnet MS/TP, vendor A (for example, a Continuum bCX1-R)
7 BACnet router between BACnet/IP and BACnet MS/TP, vendor C
8 BACnet MS/TP network
9 BACnet MS/TP device (for example, a Continuum b3 field controller)
10 BACnet Modicon M168 controller with the TM168BACS connectivity module
11 BACnet Modicon M168 controller with the TM168BACW connectivity module

Master-Slave/Token Passing (BACnet MS/TP)

Modicon M168 controllers can be connected to a BACnet Building Management System (BMS) on an RS-485 network. BACnet MS/TP Modicon M168 controllers connect via serial communications to a BACnet router, which in turn communicates over Ethernet to a B-OWS. The B-OWS communicates via Ethernet with a BACnet/IP BMS controller:

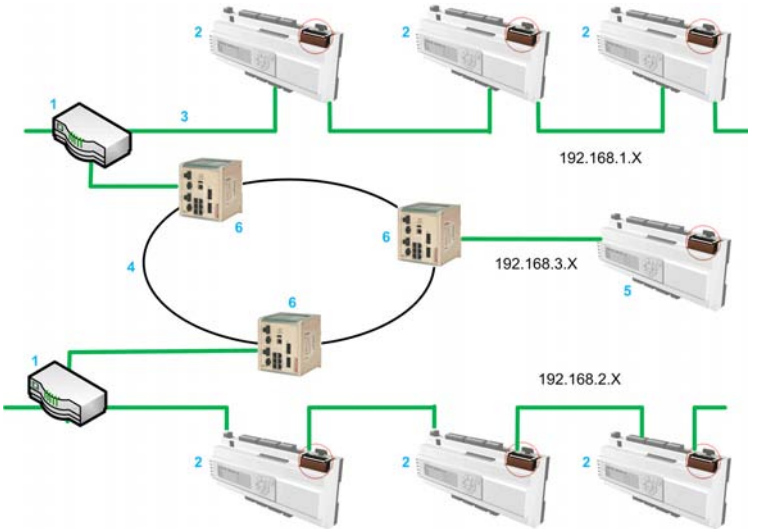


1 B-OWS (for example, a Continuum CyberStation)
2 BACnet/IP network
3 BACnet router between BACnet/IP and BACnet MS/TP (for example, a Continuum bCX1-R)
4 BACnet MS/TP device (for example, a Continuum b3 field controller)
5 SoHVAC software
6 BACnet Modicon M168 controller with TM168BACS module inside
7 BACnet MS/TP network

NOTE: Modicon M168 controllers operate as a master node on a BACnet MS/TP network (device address 0 ... 127).

Internet Protocol (BACnet/IP)

BACnet/IP controllers from Schneider Electric can be connected directly to an Ethernet backbone so that the B-OWS software communicates directly to each controller. BMS controllers with Ethernet capability can read status and perform control tasks by communicating on the Ethernet network to each controller. Here is an example of such a network.



1 BACnet Broadcast Management Device (BBMD) (for example, the Continuum CyberStation from Schneider Electric)
2 BACnet Modicon M168 controller with the TM168BACW connectivity module
3 BACnet/IP network
4 Internet
5 TM168BACW foreign device
6 Network switch or router (for example, a ConneXium switch from Schneider Electric)

NOTE: A foreign device *(see page 164)* is a BACnet device with an IP subnet address that is different from the subnet address of the BACnet/IP network that the device seeks to join.

4.2 Wiring of the BACnet MS/TP Communication Network

Overview

This section describes how to connect a TM168BACS module to a BACnet MS/TP network and describes the available network topology.

What Is in This Section?

This section contains the following topics:

Topic	Page
Cable Requirements for BACnet MS/TP Networks	54
BACnet Standard 9.2	55
Shielding	57
BACnet MS/TP Network Configurations	59

Cable Requirements for BACnet MS/TP Networks

Description

BACnet MS/TP is a master-slave token-passing local area network (LAN) fieldbus. This protocol supports a combination of shared resource and peer-to-peer communications, where more than one device can be the network master at any given time.

Electrically, BACnet MS/TP adheres to standard RS-485 and is physically wired using a two-conductor shielded twisted-pair cable.

RS-485 Cable Specifications

Cables used to create the RS-485 network should conform to these specifications:

Cable Type	twisted-pair, copper wire, tinned **NOTE:** Use 60/75 or 75 °C copper (CU) wire only, 14-30AWG.
Shield	braid
Nominal Impedance	100-120 Ω
Velocity of Propagation	78%
Capacitance	< 41.0105 pF/m (12.5 pF/ft) between conductors
	< 72.1784 pF/m (22 pF/ft) between the conductor connected to ground and the next conductor

Maximum Cable Length

Cable lengths of up to 1200 m (4000 ft) daisy chained from device to device are supported. A signal repeater is required after 1200 m (4000 ft) to add more nodes to the network (as specified, below) or further extend the cabling. A fiber repeater is recommended for running cables between buildings and through environments prone to electrical interference.

Repeater Connections

The physical length may be extended by using RS-485 or fiber repeaters. Schneider Electric offers a b-Link RS485 repeater and a b-Link (F) Fiber repeater.

BACnet Standard 9.2

Introduction

This topic summarizes BACnet standard 9.2.

Cabling

BACnet MS/TP networks use shielded, twisted-pair cables:

impedance	between 100 Ω and 130 Ω
maximum recommended segment length	1200 m (4000 ft) with 0.82 mm^2 conductor area (AWG 18) cables*
*Longer distances and/or different wire gauges comply with EIA-485 electrical specifications.	

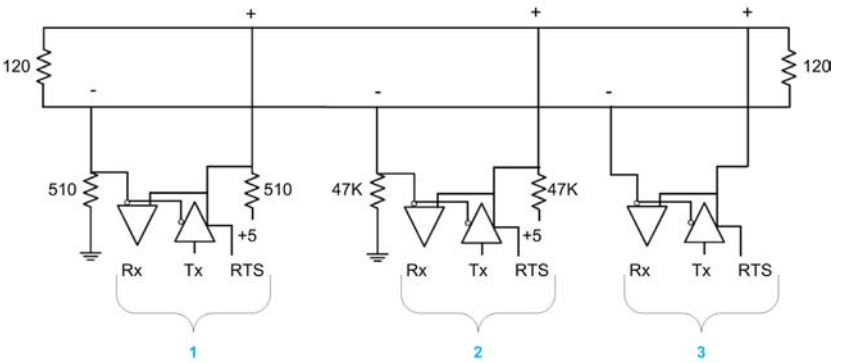
Connections

In accordance with EIA-485, the maximum number of nodes permitted per segment is 32. Repeaters allow for the connection of additional nodes. The polarity of cable connections is important due to the fact that BACnet MS/TP uses NRZ encoding.

NOTE: The network connectivity modules for Modicon M168 controllers represent half of the standard load, so 64 devices can be connected per segment.

Terminations

BACnet MS/TP EIA-485 networks do not have T connections. Terminator resistors of 120 Ω ±5% are connected to both ends of the segment. Do not use other terminator resistors at intermediate nodes. This graphic shows an EIA-485 network with three types of nodes:

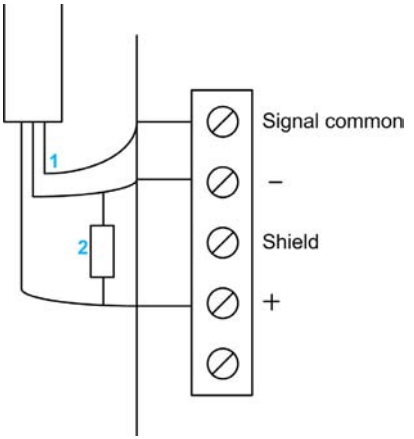


1 node with network bias resistors
2 node with local bias resistors
3 node without bias resistors

NOTE: The Modicon M168 modules are examples of node type 3: nodes without bias resistors.

RS-485 Termination

The BACnet MS/TP fieldbus requires a 120 Ω terminator resistor at both ends of a daisy chain segment. Place the terminator resistors as close as possible to the modules at the end of the chain. Here is an example of the connection of the terminator:



1 Signal common
2 TSCAR01NM120 or any wired terminator resistor of 120 Ω ± 5%

Shielding

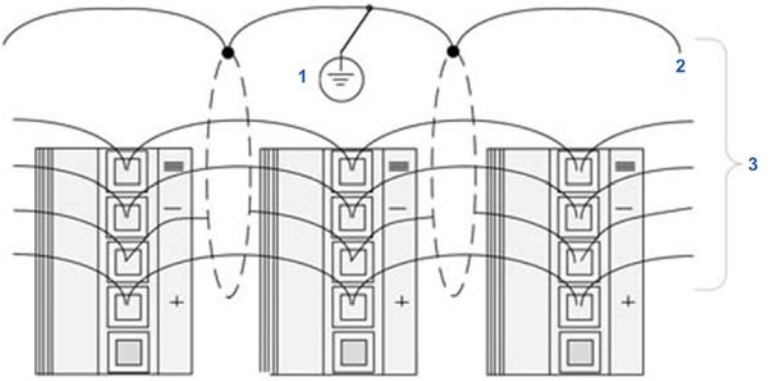
Description

This topic describes how to apply shielding to BACnet MS/TP networks and provides reference examples.

RS-485 Network Shielding

The shield within the RS-485 cable helps protect the network from electromagnetic interference and harmful transient voltage spikes. A properly applied shielding strategy can lead to more reliable communications. Connect each device on the RS-485 network to the shield. To facilitate this, the middle pin on the five-position terminal block provides the shield connection. The RS-485 cables, which Schneider Electric sells for Profibus DP, can also be used with BACnet MS/TP.

Refer to this diagram for the wiring details of network connectivity modules in a 3-wire RS-485 system:



1 grounded shield
2 shield
3 to next device

Connect the shield to the protective ground (PE) at only one point along the RS-485 network. BACnet MS/TP devices in the network are coupled to PE only capacitively. Do not tie them to PE.

The automation network shield should be grounded in only one place, typically at the RS-485 converter. Grounding the shield at multiple points creates a ground loop that may disrupt communication or cause damage to the controller circuitry.

NOTICE

GROUND LOOP

Properly ground the shield at only one point in the system, as indicated in this documentation.

Failure to follow these instructions can result in equipment damage.

BACnet MS/TP Network Configurations

Description

With BACnet MS/TP, use a daisy chain networking topology. Star and ring networks are not supported.

Daisy Chain Configuration

Daisy chain configurations consist of a single cable that is routed to the first BACnet MS/TP device, the next device, and so on in the sequence.

Address Range and Number of Nodes

The BACnet MS/TP network supports 256 nodes (address range 0...255):

- Addresses 0 to 127 are reserved for BACnet master devices (for example, the TM168BACS module).
- Addresses 128 to 255 are reserved for BACnet slave devices.

A BACnet MS/TP network can support up to 32 full-load nodes per network segment. The load of a node can vary. For example, the TM168BACS module uses only a half-load.

Thus, if four TM168BACS modules are placed in the same network segment, their combined load is the equivalent of:

(4 nodes) x (0.5 load/node) = 2 loads.

In this case, the network segment could support these additional nodes:

- 30 full-load nodes
- 60 half-load nodes

The maximum distance between devices on the BACnet MS/TP network is 1200 m (4000 ft) before a repeater is needed. Terminators (120 Ω) are required at both ends of the network.

4.3 Wiring of the Ethernet Communication Network

Overview

This section describes how to connect a Modicon M168 controller to an Ethernet network using an RJ45 connector on a TM168BACW or TM168MODW connectivity module. It also describes the available network topologies.

What Is in This Section?

This section contains the following topics:

Topic	Page
Port Characteristics and Wiring	61
Ethernet Network Connection	63

Port Characteristics and Wiring

Description

These are the main physical characteristics of an Ethernet port:

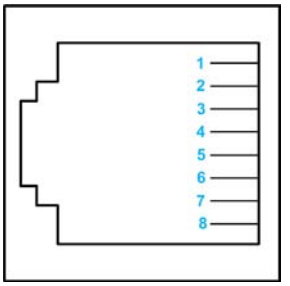
Physical Interface	Ethernet 10/100BASE-T
connector	RJ45
transmission speed	10/100 Mbps (full- or half-duplex)

Physical Interface and Connectors

The TM168BACW and TM168MODW connectivity modules have 2 female shielded RJ45 connectors:

RJ45 Ethernet Network Connector Pinout

The Modicon M168 controller is connected to the Ethernet network using either or both RJ45 Ethernet ports. This port complies with these wiring specifications:

Front View	Pin Number	Signal	Pair	Description
	1	TD+	A	Transmit +
	2	TD-	A	Transmit -
	3	RD+	B	Receive +
	4	Do not connect.	—	—
	5	Do not connect.	—	—
	6	RD-	B	Receive -
	7	Do not connect.	—	—
	8	Do not connect.	—	—

Auto-MDIX

Each RJ45 connector provides a media-dependent interface crossover (MDIX) connection. Each port automatically senses these characteristics:

- cable type, straight or crossed, plugged into the connector, and
- pin requirements of the device to which the controller is connected

Using this information, each connector assigns transmit and receive functions to pin combination 1/2 and pin combination 3/6 as necessary to communicate with the device on the other end of the cable.

NOTE: Auto-MDIX lets you use a straight or crossed category 5 twisted pair Ethernet cable to connect a Modicon M168 controller to another device.

Ethernet Network Connection

Connection to the Network

Every TM168BACW and TM168MODW Ethernet connectivity module provides the Modicon M168 controller with an embedded 2-port Ethernet switch, which permits flexible network design. Ethernet network topologies include:

- star
- daisy chain
- ring, using a Schneider Electric ConneXium switch that supports HiPER-Ring configurations

The controller complies with the IEEE 802.3 standard for Ethernet.

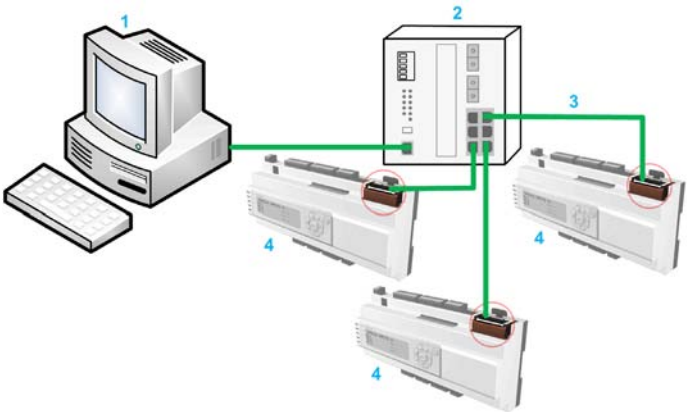
Network Characteristics

Designation	Description
type of cable	straight or crossed category 5 shielded twisted pair
maximum cable length	100 m (328 ft)

NOTE: To reduce interference, keep the Ethernet cable away from the power cables (at least 30 cm (12 in.)). If necessary, create crossovers of the Ethernet cable and the power cables at right angles.

Star Topology

In a star topology, each Modicon M168 controller connects to an external switch:

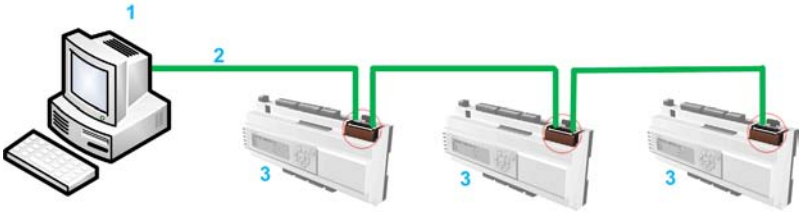


1 BACnet operator workstation (B-OWS) or Modbus TCP client, in this case a Continuum CyberStation from Schneider Electric
2 ConneXium switch
3 straight or crossed category 5 shielded twisted pair Ethernet cable with RJ45 connector

4 Modicon M168 controller with Ethernet module inside

Daisy Chain Topology

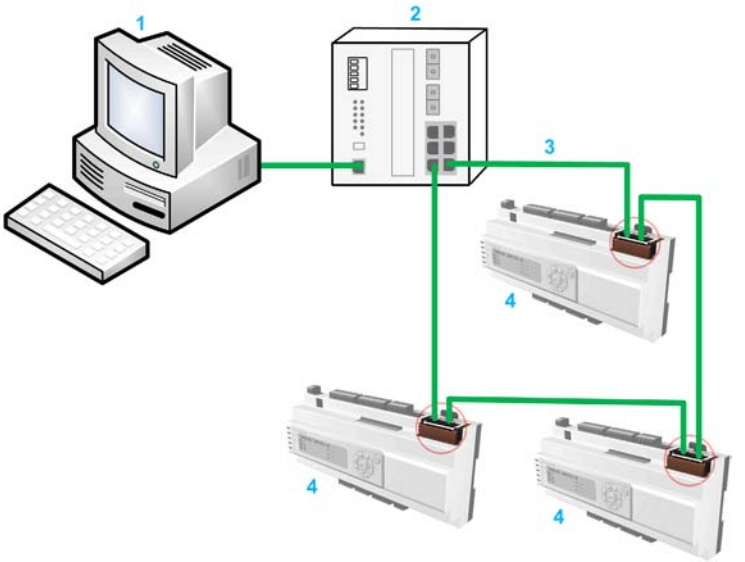
Because every Modicon M168 controller with an Ethernet module installed includes a 2-port embedded Ethernet switch, the daisy chain topology requires no switches or hubs between controllers for collisionless communication:



1 BACnet operator workstation (B-OWS) or Modbus TCP client, in this case a Continuum CyberStation from Schneider Electric
2 straight or crossed category 5 shielded twisted pair Ethernet cable with RJ45 connector
3 Modicon M168 controller with an Ethernet connectivity module

Ring Topology

A ring topology is a daisy chain where the last controller in the chain loops back to the central switch. The ring topology provides redundancy. When network communications break at any single point, the network segment on each side of the break continues to operate as if the network was designed as a 2-star or daisy chain topology:



1 BACnet operator workstation (B-OWS) or Modbus TCP client, in this case a Continuum CyberStation from Schneider Electric
2 ConneXium managed switch
3 straight or crossed category 5 shielded twisted pair Ethernet cable with RJ45 connector
4 Modicon M168 controller with an Ethernet connectivity module

Schneider Electric ConneXium switches with HiPER-Ring technology include:

- 499NxSxxx: In its default configuration, switch ports 6 and 7 support HiPER-Ring design.
- TCSESMxxx: By default, no switch ports support hyper-ring design. Consult the switch user manual and web pages for information on how to configure selected switch ports for HiPER-Ring configurations.

Commissioning

5

Overview

This chapter shows you how to add your network connectivity module to your Modicon M168 controller and how to configure the module settings.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
5.1	Commissioning Communications	68
5.2	Exporting Variables from SoHVAC	84

5.1 Commissioning Communications

Introduction

Use the SoHVAC configuration software to configure the Modicon M168 connectivity modules for communications.

What Is in This Section?

This section contains the following topics:

Topic	Page
Select the Controller and Configure the TM168BACS Module	69
Select the Controller and Configure the TM168BACW Module	74
Select the Controller and Configure the TM168MODW Module	78

Select the Controller and Configure the TM168BACS Module

Introduction

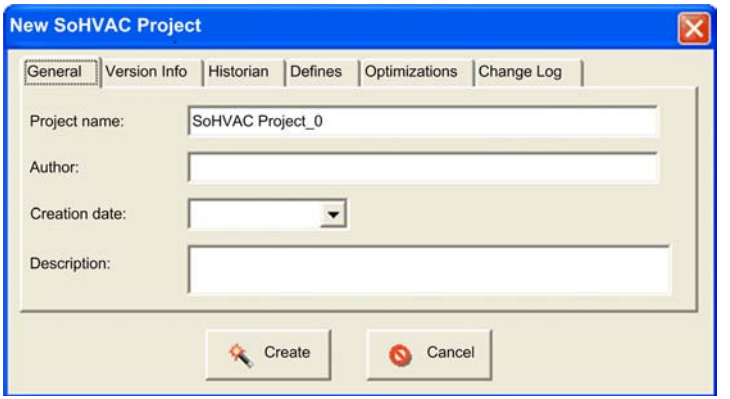
This section describes the use of the SoHVAC configuration software to configure the TM168BACS module for BACnet MS/TP communications:

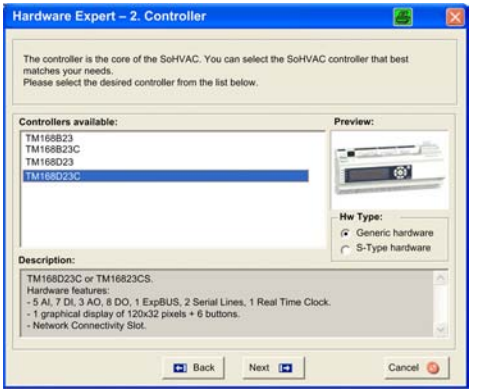
Stage	Description
1	Select the controller and the TM168BACS module.
2	Configure the TM168BACS module.

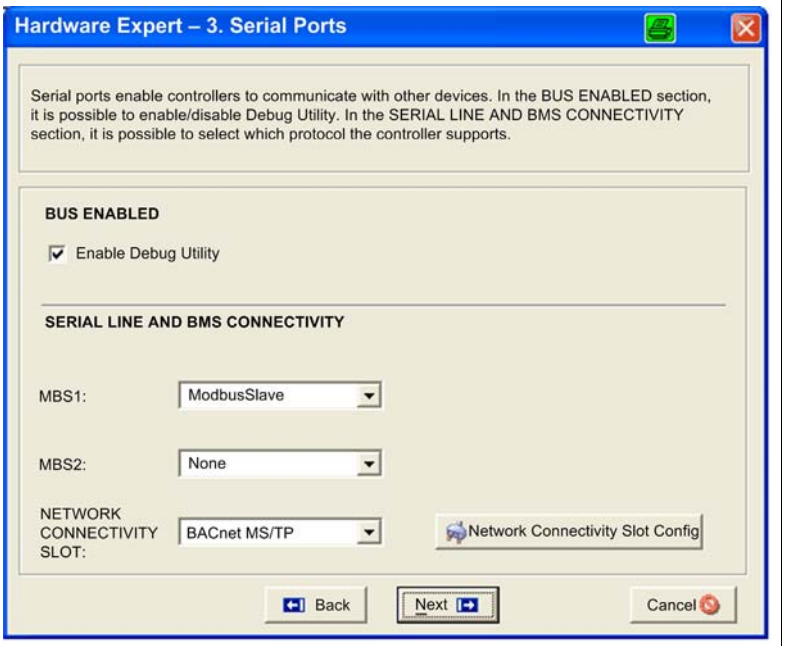
NOTE: By default, BACnet communications are disabled for all controllers. Only one of the BACnet networks can be enabled at a time. For example, BACnet/IP is disabled when BACnet MS/TP is enabled (and vice versa).

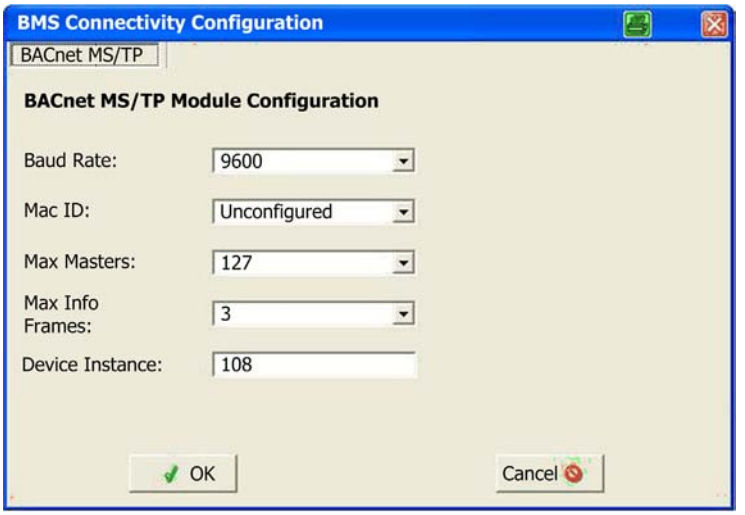
Procedure

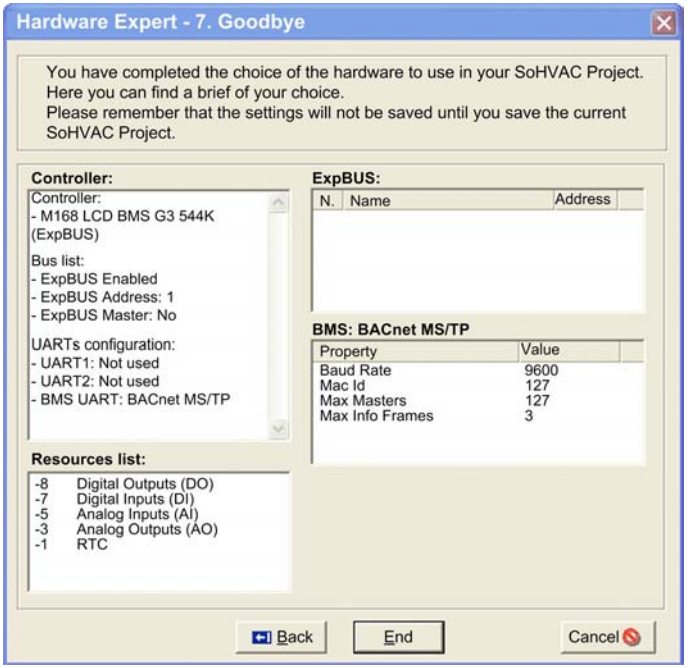
Configure your module and Modicon M168 controller for BACnet MS/TP communications.

Step	Action
1	Create a new project (**File** → **New Project**).
2	In the **New SoHVAC Project** dialog, enter the author name, the date, and the (optional) brief description of the project. Click **Create** to apply these settings to your project. 
3	Open the **Hardware Expert** (**Project** → **Hardware Expert**).

Step	Action
4	In the **Hardware Expert** dialog box, click **Next**.
5	In the **Controller** dialog, select the appropriate controller and click **Next**. 

Step	Action
6	In the **Serial Ports** dialog, use the **BMS** dropdown menu to select the **BACnet MS/TP** protocol for your network connectivity module and click **Config**:  **NOTE:** The module protocol defaults to **None**.

Step	Action
7	The **BMS Connectivity Configuration** screen opens: 
8	Set the **Baud Rate** using the dropdown menu. (Supported baud rates for BACnet MS/TP are 9600, 19200, 38400, and 76800.)
9	Enter a **Mac ID** value (1 ... 127) from the dropdown menu. (By default, the **Mac ID** is set to **Unconfigured**.)
10	Enter the **Max Masters** value (1 ... 127) from the dropdown menu.
11	Enter a **Max Info Frames** value (1 ... 3) from the dropdown menu and click **OK** to close the **BMS Connectivity Configuration** dialog box.
12	Enter a **Device Instance** value (1 ... 4194303) and click **OK** to return to the **Serial Ports** dialog.
13	In the **Serial Port** dialog, click **Next**. .
14	The **Expansions** dialog box opens. The steps in this dialog do not relate to communications, but they are necessary for you to complete the configuration of your module. Update the screen according to your application needs and click **Next**.
15	The **User Interfaces** dialog opens. The steps in this dialog do not relate to communications, but they are necessary for you to complete the configuration of your module. Update the screen according to your application needs and click **Next**.
16	The **Network ExpBUS** dialog opens. The steps in this dialog do not relate to BMS communication, but they are necessary for you to complete the configuration of your module. Update the screen according to your application needs and click **Next**.

Step	Action
17	A summary screen allows you to view and confirm your configuration choices. Take one of these actions: ● Click **Back** to make additional configuration changes. ● Click **End** to apply your configuration choices. The dialog box closes. All settings are saved and the controller reboots. If BACnet/IP was previously enabled, it is automatically disabled. ● Click **Cancel** to close the **Hardware Expert** without applying your configuration choices.  **NOTE:** ExpBUS is shown in this **Hardware Expert** example, but it is only one of several options.

Select the Controller and Configure the TM168BACW Module

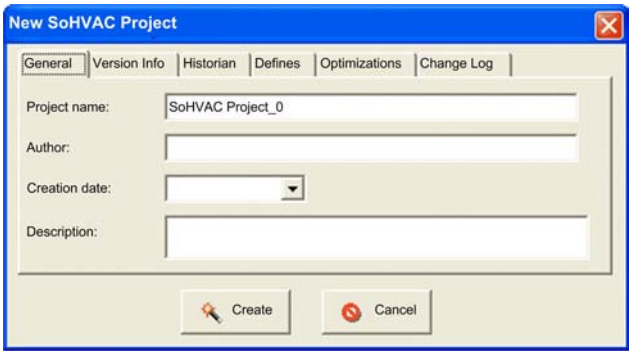
Introduction

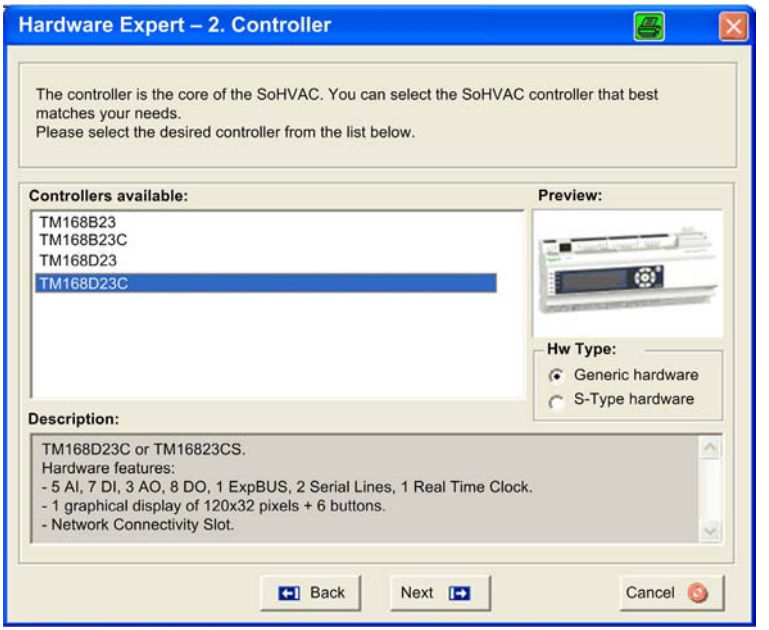
This section describes the selection of controller and TM168BACW module using the SoHVAC software.

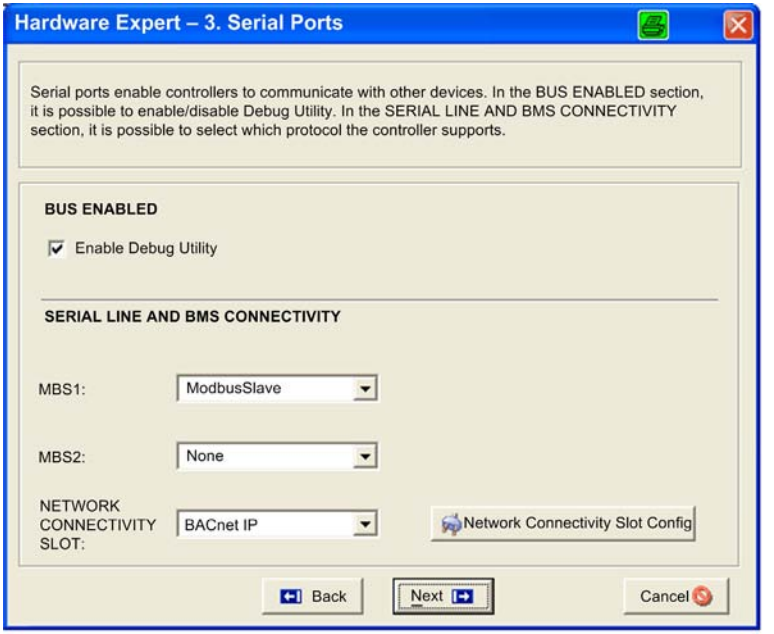
NOTE: The network parameters of the module are configured using the embedded web pages *(see page 104)*.

Description

The first step for commissioning your BACnet/IP module is to open SoHVAC. After SoHVAC is open, start the commissioning:

Step	Action
1	Create a new project: **File** → **New Project**
2	In the **New SoHVAC Project** dialog, enter the author name, the date, and the (optional) brief description of the project. Click **Create** to apply these settings to your project:  Enter the author name, the date, and the (optional) brief description of the project. Click **Create** to apply this information to your project.
3	Open the **Hardware Expert**: **Project** → **Hardware Expert**

Step	Action
4	In the **Hardware Expert** dialog box, click **Next**:
5	In the **Controller** dialog, select the appropriate controller and click **Next**: 

Step	Action
6	In the **Serial Ports** dialog, view the available protocol choices in the dropdown menu. Select the protocol for your network connectivity module and click **Next**:  **NOTE:** The module protocol defaults to **None**.
7	The **Expansions** dialog box opens. The steps in this screen do not relate to BMS communications, but they are necessary for you to complete the configuration of your module. Update the screen according to your application needs and click **Next**.
8	The **User Interfaces** dialog opens. The steps in this screen do not relate to BMS communications, but they are necessary for you to complete the configuration of your module. Update the screen according to your application needs and click **Next**.
9	The **Network ExpBUS** dialog opens. The steps in this screen do not relate to BMS communications, but they are necessary for you to complete the configuration of your module. Update the screen according to your application needs and click **Next**.

Step	Action

10	A summary screen lets you view and confirm your selections. Take one of these steps:
	● Click **Back** to make additional configuration changes.
	● Click **End** to apply your configuration choices. The dialog closes, and these events occur:
	  ● All settings for the TM168BACW module are saved,
	  ● If BACnet MS/TP was previously enabled, it is automatically disabled.
	  ● If the TM168BACW module has already been inserted into the controller, both the module and the controller reboot.
	NOTE: When the TM168BACW module first powers up, it automatically installs the web pages for the controller. During this first initialization (which can take several minutes) the module status (MS) LED alternately flashes red/green. This delay occurs only for the first power cycle. Wait for the MS LED to stop flashing before you access the embedded web pages for the controller.
	● Click **Cancel** to close the **Hardware Expert** without saving your edits.
	
	NOTE: ExpBUS in the **Hardware Expert** example is only one of several options.

You can now configure the module with the embedded web pages *(see page 91)*.

Select the Controller and Configure the TM168MODW Module

Introduction

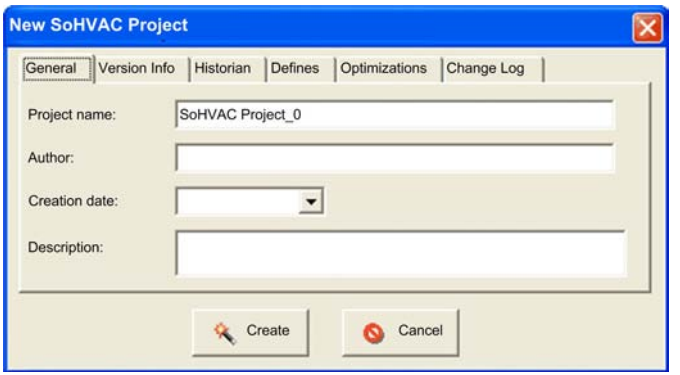
The TM168MODW communication module has a factory-installed default configuration. You can configure the module with the SoHVAC **Hardware Expert** through this process:

Stage	Description
1	Create a new SoHVAC project.
2	Select the Modicon M168 controller.
3	Configure the connectivity.
4	View the configuration summary.

These stages are described in detail below.

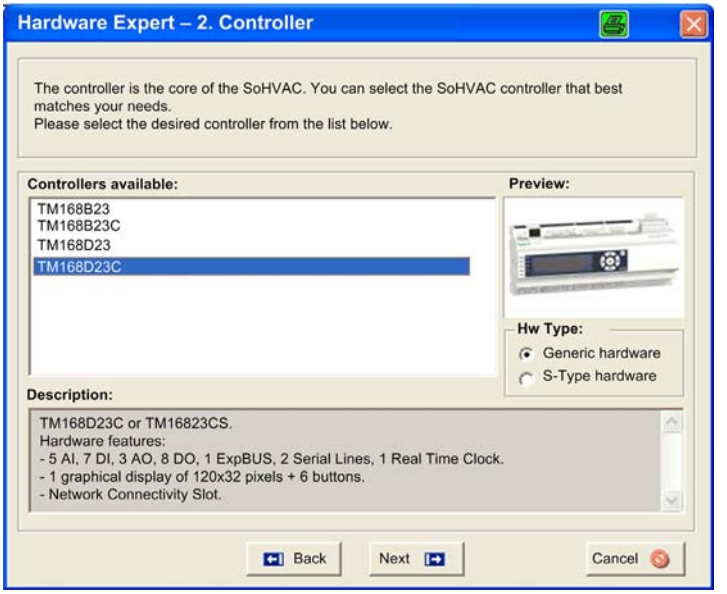
Create a New SoHVAC Project

Create a new SoHVAC project:

Step	Action
1	Open SoHVAC.
2	Create a new project: **File** → **New Project**
3	The **New SoHVAC Project** dialog box appears. Enter an author name, the date, and the (optional) brief description of the project: 
4	Click **Create** to apply the new project settings.

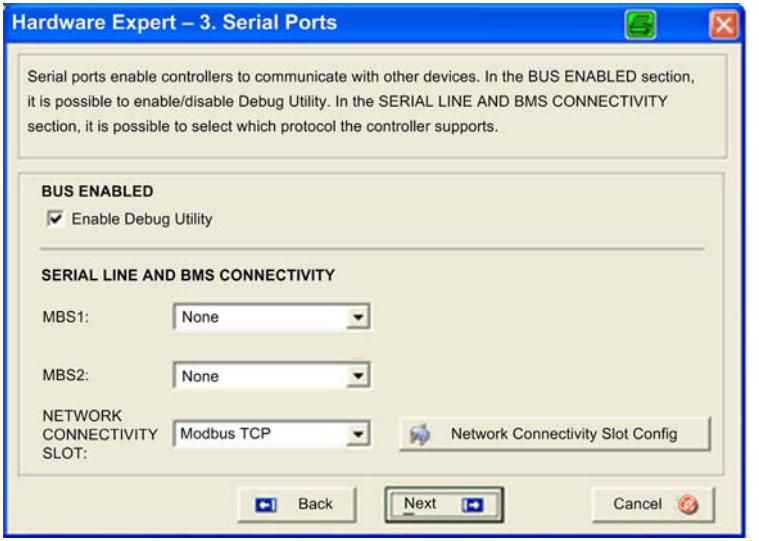
Select the Modicon M168 Controller

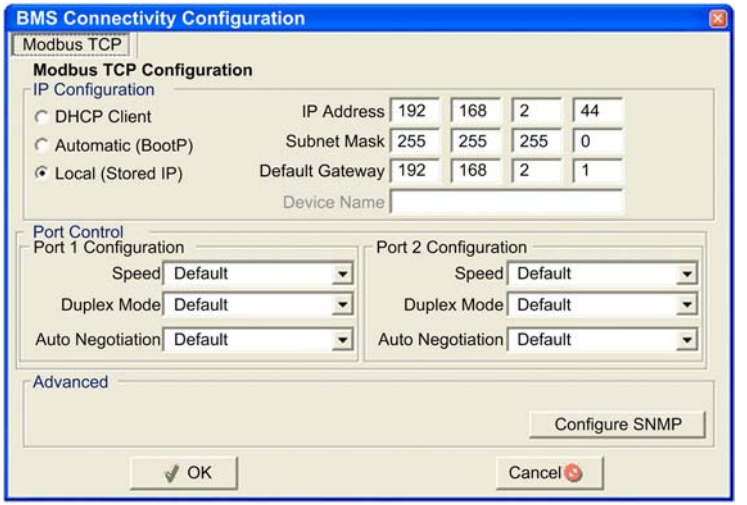
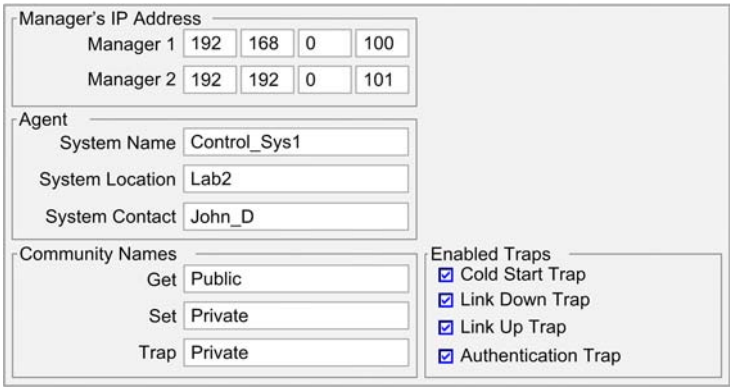
Select your controller:

Step	Action
1	Open the SoHVAC **Hardware Expert**: **Project** → **Hardware Expert**
2	When the **Welcome** screen appears, click **Next**:
3	When the **Controller** dialog appears, select the appropriate controller and click **Next**: 

Configure Connectivity

You can now see the **Serial Ports** dialog box.

Step	Action
1	Select the protocol for your network connectivity module in the **Serial Ports** dialog box:  **NOTE:** Check **Enable Debug Utility** to debug your application.
2	Click **Network Connectivity Slot** in the **Serial Ports** dialog box. The **BMS Connectivity Configuration** dialog box appears.

Step	Action
3	Configure the parameters:  **NOTE:** Elsewhere in this guide are descriptions for the individual IP parameters *(see page 107)* and port configuration parameters *(see page 114)*.
4	Click **Configure SNMP** to open the configuration window for the SNMP Agent:  **NOTE:** The SNMP parameters are described elsewhere in this document *(see page 111)*.
5	Click **OK** to return to the **BMS Connectivity Configuration** screen.
6	When the **BMS Connectivity Configuration** dialog box appears, click **OK**.

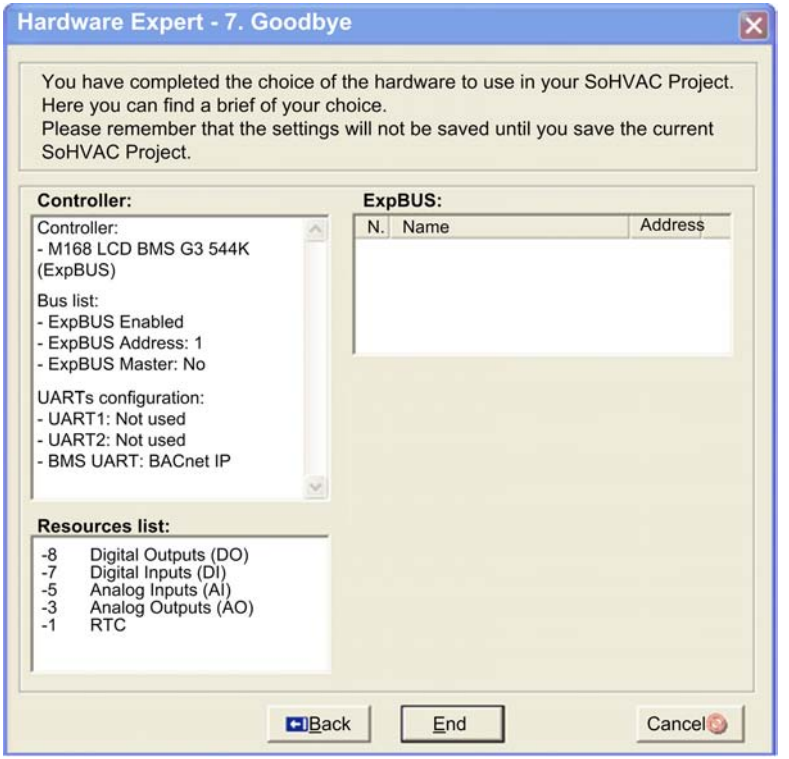
Update the required information:

Step	Action
1	In the **Hardware Expert** screen, click **Next**.
2	The **Expansions** dialog box appears. Update the screen in accordance with your application needs and click **Next**. (See the note below.)
3	The **User Interfaces** dialog appears. Update the screen according to your application needs and click **Next**. (See the note below.)
4	The **Network ExpBUS** dialog appears. Update the screen according to your application needs and click **Next**. (See the note below.)

NOTE: The steps in these screens do not relate to BMS communication, but they are required for the completion of the module configuration.

View the Configuration Summary

A summary screen appears:



NOTE: ExpBUS is one of several options.

Click a button:

- **Back:** Make additional configuration changes.
- **End:** Apply your configuration choices. The dialog closes and these events occur:
  - All settings for the TM168MODW module are saved.
  - If Modbus TCP was previously enabled, it is automatically disabled.
  - If the TM168MODW module has already been inserted into the controller, the module and the controller both reboot.

  NOTE: When the TM168MODW module first powers up, it automatically installs the web pages for the controller. During this first initialization (which can take several minutes) the module status (MS) LED alternately flashes red/green. This delay occurs only for the first power cycle. Wait until the MS LED stops flashing before accessing the embedded web pages for the controller.
- **Cancel:** Close the **Hardware Expert** without saving your changes.

You can now configure the module with the embedded web pages *(see page 91)*.

5.2 Exporting Variables from SoHVAC

Introduction

This section tells you how to export variables from SoHVAC to the communication module for Modicon M168 controllers.

What Is in This Section?

This section contains the following topics:

Topic	Page
Exporting Variables From SoHVAC to a Modbus TCP Module	85
Exporting Variables from SoHVAC to a BACnet Module	87

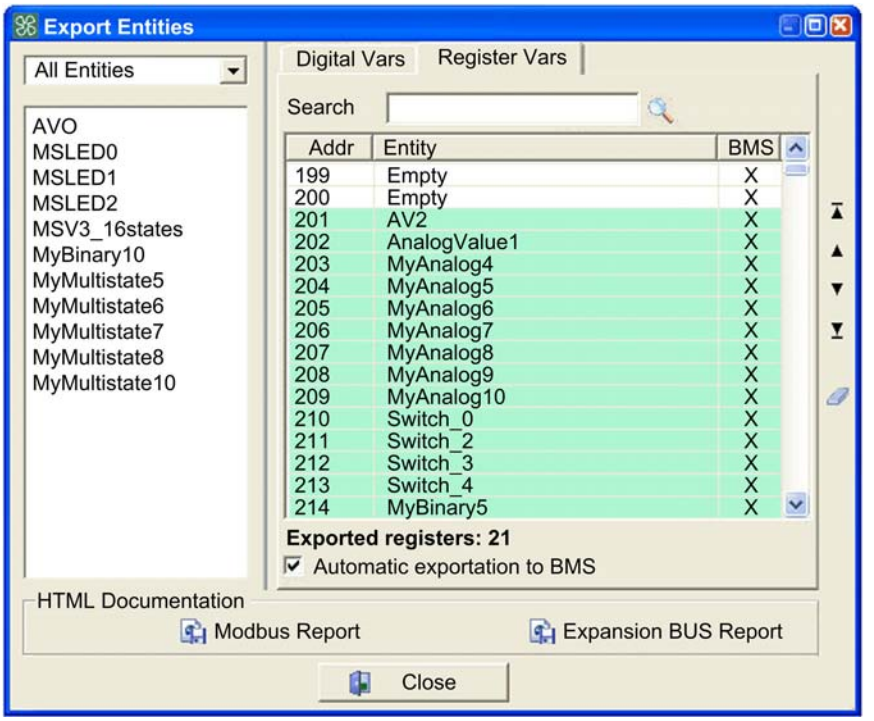
Exporting Variables From SoHVAC to a Modbus TCP Module

Introduction

Read or write variables with Modbus TCP by exporting the variables with the SoHVAC **Export Entities** command.

Export Screen

From the SoHVAC **Tools** menu, scroll to **Export Entities**. The **Export Entities** dialog box appears:



⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not export critical application parameters that would result in remote write access unless you have performed a thorough analysis of the implications of unintended remote access.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

All variables are exported to the Modbus serial ports of the module, but you can also choose to export all variables to the Modbus TCP (BMS) port of the module by checking **Automatic Exportation to BMS**.

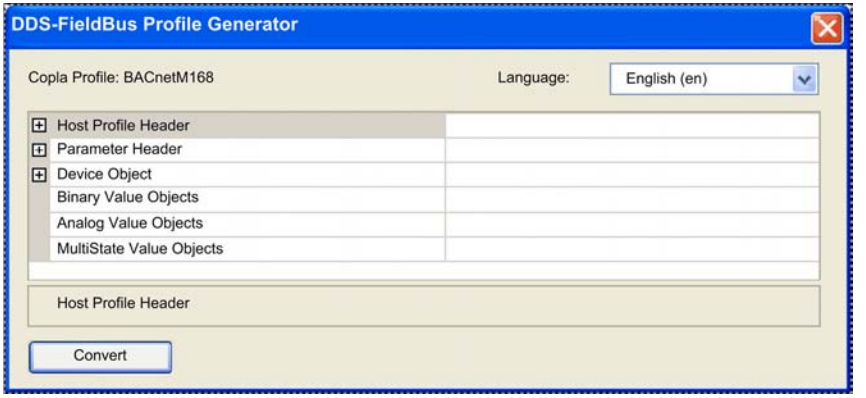
To control individual exported variables, do not check **Automatic Exportation to BMS**. Instead, right-click the variable in the **Export Entities** window and scroll to one of these commands:

- **Export to BMS:** Export the selected variable to the Modbus TCP port of the module.
- **Remove from BMS:** Remove the selected variable from the Modbus TCP port of the module.

Exporting Variables from SoHVAC to a BACnet Module

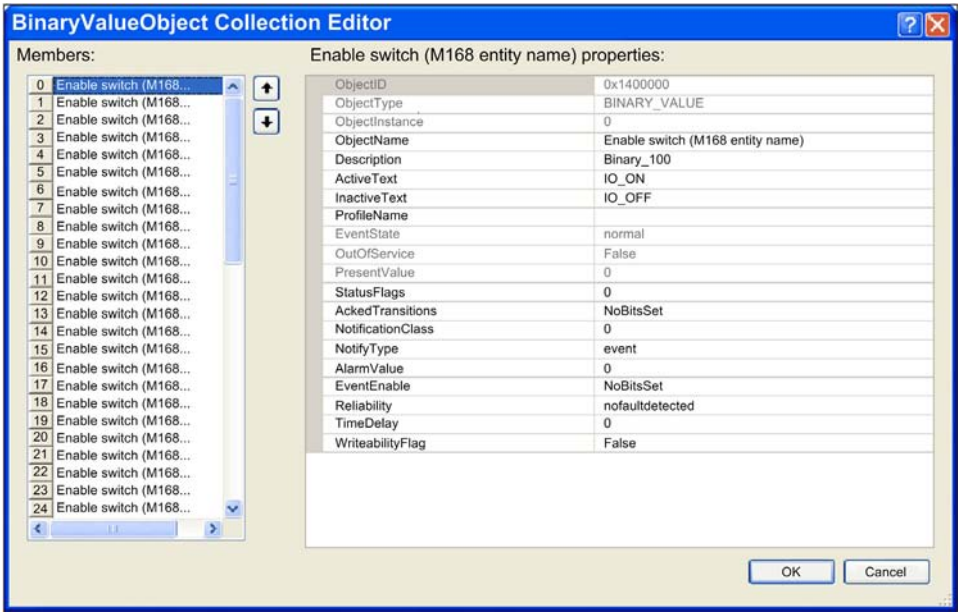
Description

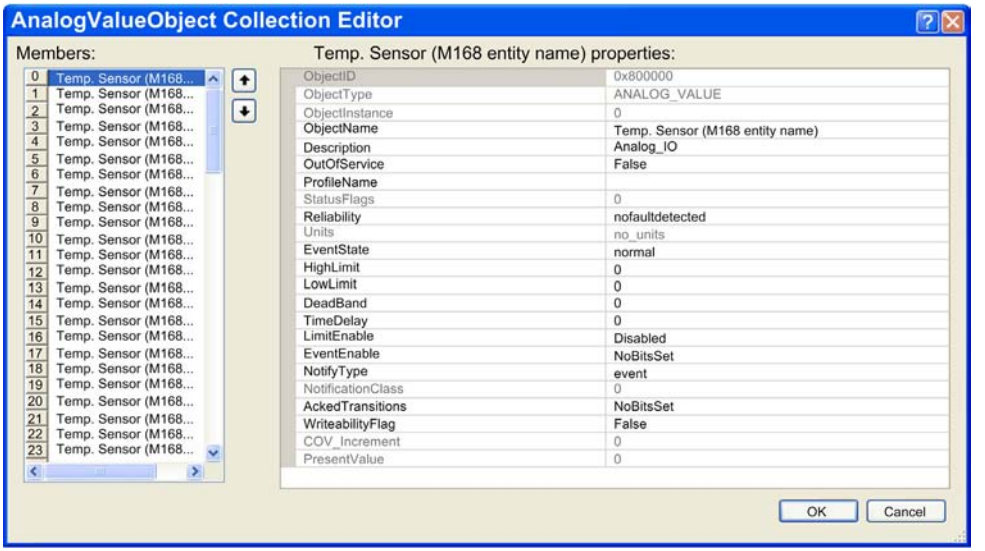
The **Fieldbus Profile Generator** allows you to export variables from SoHVAC to BACnet.

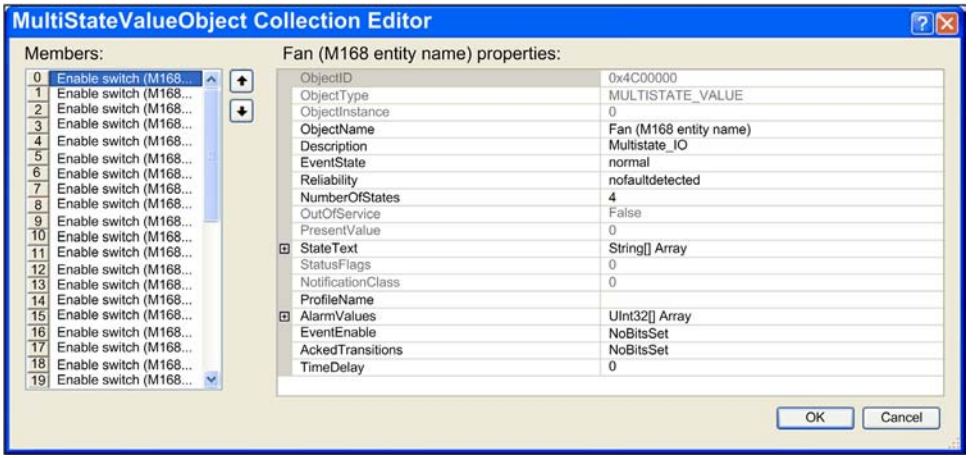
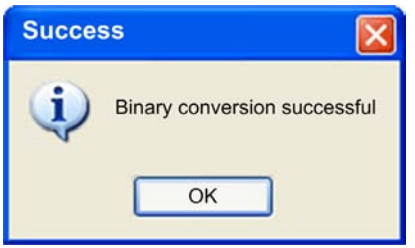


Exporting Variables

Host Profile Header and **Parameter Header** are included for your reference. Expand the headings to view the read-only values.

Step	Action
1	Expand the **Device Object** list to view related values. You can edit values that are not grayed out.
2	Select **Binary Value Objects** and click the ellipsis [...] to open the **BinaryValueObject Collection Editor**:  **NOTE:** The maximum number of variables exported depends upon the size of the variables. Exporting more than 300 variables is possible if you limit the number of multi-state value (MSV) objects to 16. The FPG indicates if you are exporting too many variables during the profile generation process.
3	Select a member (0...59) and change the editable values as desired. Click **OK** to accept your changes and return to the **Fieldbus Profile Generator** screen.

Step	Action
4	Select **Analog Value Objects** and click the ellipsis [...] to open the **AnalogValueObject Collection Editor**:  **NOTE:** The maximum number of variables exported depends upon the size of the variables. Exporting more than 300 variables is possible if you limit the number of MSV objects to 16. The FPG indicates if you are exporting too many variables during the profile generation process.
5	Select a member (0...99) and change the editable values as desired. Click **OK** to accept your changes and return to the **Fieldbus Profile Generator** screen.

Step	Action
6	Select **Multi-State Value Objects** and click the ellipsis [...] to open the **MultiStateValueObject Collection Editor**:  **NOTE:** The maximum number of variables exported depends upon the size of the variables. Exporting more than 300 variables is possible if you limit the number of MSV objects to 16. The FPG indicates if you are exporting too many variables during the profile generation process.
7	Select a member (0...39), and change the editable values as desired. Click **OK** to accept your changes and return to the **Fieldbus Profile Generator** screen.
8	Click the **Convert** button to finalize your changes. A message confirms your changes: 
9	Click **OK**.

Using the Embedded Web Pages

6

Overview

This chapter describes the embedded web pages for the TM168BACW and TM168MODW modules. It includes these instructions:

- Access web pages.
- Configure the module through web pages.
- Diagnose the module through web pages.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
6.1	Connecting to the Module for the First Time	92
6.2	The Embedded Web Pages	96
6.3	Configuring the Modicon M168 Ethernet Modules	104
6.4	Monitoring and Diagnosing the Status of the Modicon M168 Ethernet Module	116
6.5	Customizing Modicon M168 Connectivity Module Web Pages	128

6.1 Connecting to the Module for the First Time

Connecting to the Module

Before You Begin

Before connecting to a TM168BACW or TM168MODW module for the first time, take these steps:

- Determine the IP configuration settings of the Modicon M168 controller, which is configured through the SoHVAC software. The IP configuration of the Modicon M168 con can be determined using the controller build (**Networks** → **BMS**).
- Determine if there is a BootP server on the network that is pre-configured to deliver settings to the module. If so, find out the IP address that will be assigned to the module by the BootP server.
- If there is no BootP server, determine the Ethernet MAC address-based default IP address for the module.
- After the initial IP address of the module is determined, check that the IP address of the PC is configured so that your PC and the module are part of the same subnet. If necessary, you can temporarily assign a static IP address to your PC *(see page 93)*.
- Using an Ethernet cable, connect your PC to the module, either directly or indirectly (for example, through an Ethernet switch).

BootP

When the TM168BACW or TM168MODW connectivity module is first powered up, it automatically sends a BootP request for configuration settings. If a BootP server exists on the network with settings for the module, those configuration settings (including the IP address assigned to the module) are transmitted to the module.

NOTE: The BootP server contains a table that maps the Ethernet MAC address (assigned at the factory) of each network device to the IP address for that device. Before the BootP server can assign an IP address to the connectivity module, you need to make an entry in the BootP table. The entry maps the Ethernet MAC address of the module to its intended IP address. (Consult your network administrator for the IP address to be assigned to your module.)

If no BootP server exists on your network, the module waits for about 2 minutes. Then it uses its default IP address.

In either case, when the IP assignment process is complete, you can use an Internet browser to connect to the device using its new IP address.

Default IP Address

If no IP address is assigned to the module by a BootP server on initial start-up, the module uses its default IP address. The default IP address is represented as 10.10.***x***.***y***, where ***x*** and ***y*** are the last two octets of the Ethernet MAC address (MAC4 and MAC5) in decimal format. (For example, if the Ethernet MAC address of the module is `00:80:F4:01:2C:71`, the module's default IP address is `10.10.44.113`.)

Assigning a Temporary Static IP Address to Your PC

You may have to assign a temporary static IP address to your PC to put your PC and the module on the same subnet:

Windows XP:

Step	Action
1	Open the **Network Connections** window on your PC: **Start** → **Settings** → **Network Connections**
2	Open the **Properties** window: **a.** Select one of the **Local Area Connection** items. **b.** Click the right mouse button. **c.** Select **Properties**.
3	Open the **Internet Protocol (TCP/IP) Properties** dialog box: **a.** On the **General** page, select **Internet Protocol**. **b.** Click the **Properties** button.
4	In the **General** page, select **Use the following IP address**. Enter an **IP address** and **Subnet mask** that places your PC on the same subnet as the module. For example, if the module is using its default address, you can use an IP address beginning with 85.16.x.y, and a subnet mask of 255.255.255.0. **NOTE:** Assign an IP address that is unique with respect to the other devices on the subnet.
5	Click **OK** to close the dialog.
6	Click **OK** to close the **Local Area Connection Properties**.

For Windows 7:

Step	Action
1	Open the **Control Panel** on your PC: **Start** → **Control Panel**
2	Select **Network and Sharing Center**.
3	In the **Network and Sharing Center** dialog, select **Change Adapter Settings**.
4	Select the appropriate **Local Area Network** connection to open the **Local Area Network Properties** dialog.
5	In the **Network** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Step	Action
6	Enter an **IP address** and **Subnet mask** that will place your PC on the same subnet as the module. For example, if the module is using its default address, you can use an IP address beginning with 85.16.x.y, and a subnet mask of 255.255.255.0. **NOTE:** Assign an IP address that is unique with respect to the other devices on the subnet.
7	Click **OK** to close the TCP/IP properties dialog.
8	Click **OK** to close the local area connection properties dialog.

NOTE: After you finish configuring the module, you may want to undo changes to your PC's IP configuration to make it compatible with the new module configuration.

Making the Connection

Manage IP addresses to give each device on the network a unique address. Having multiple devices with the same IP address can cause unpredictable operation of your network and associated equipment.

⚠ WARNING

UNINTENTED EQUIPMENT OPERATION

- Be sure that all devices have unique addresses.
- Obtain your IP address from your system administrator.
- Confirm that the device's IP address is unique before placing the system into service.
- Do not assign the same IP address to any other equipment on the network.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: It is good practice to ensure that your system administrator maintains a record of all assigned IP addresses on the network and subnetwork, and to inform the system administrator of all configuration changes performed.

Make the initial connection to the module:

Step	Action
1	Confirm that the connectivity module is installed and running.
2	(Conditional:) If a BootP server has provided an IP address to the module, open an Internet browser. In the **URL Address** input box, type in the assigned IP address and click **Enter**. If your browser successfully connects to the module, the BootP assignment is a success. **NOTE:** • The module uses the IP address assigned by the BootP server as long as power is applied to the module. • If the module is served an IP address, the module checks to determine if the assigned address is a duplicate. If the assigned address is a duplicate address, the module remains offline.
3	(Conditional:) If the module has used its default IP address, open an Internet browser. In the **URL Address** input box, enter the default IP address and click **Enter**. **NOTE:** The network status (**NS**) LED flashes 6 times to indicate that the module is using a default IP address.
4	After you connect to the module, you can edit the configuration of the module *(see page 104)* or monitor module operations *(see page 116)*.

6.2 The Embedded Web Pages

Overview

Use the embedded web pages to perform diagnostics and configure the Modicon M168 controller for connectivity.

What Is in This Section?

This section contains the following topics:

Topic	Page
Introducing the Web Browser	97
Accessing the Embedded Web Pages	99
Navigating the Embedded Web Pages (TM168BACW)	101
Navigating the Embedded Web Pages (TM168MODW)	103

Introducing the Web Browser

Introduction

Access the embedded web pages for the TM168BACW and TM168MODW modules through a web browser.

The embedded web pages allow this functionality for the communications module:

- **configuration:** These pages allow you to configure parameters for several module services.
- **maintenance/diagnostics:** These pages allow network diagnostics for the module services.

Use the **Help** link on each page to access context-sensitive help.

Browser Requirements

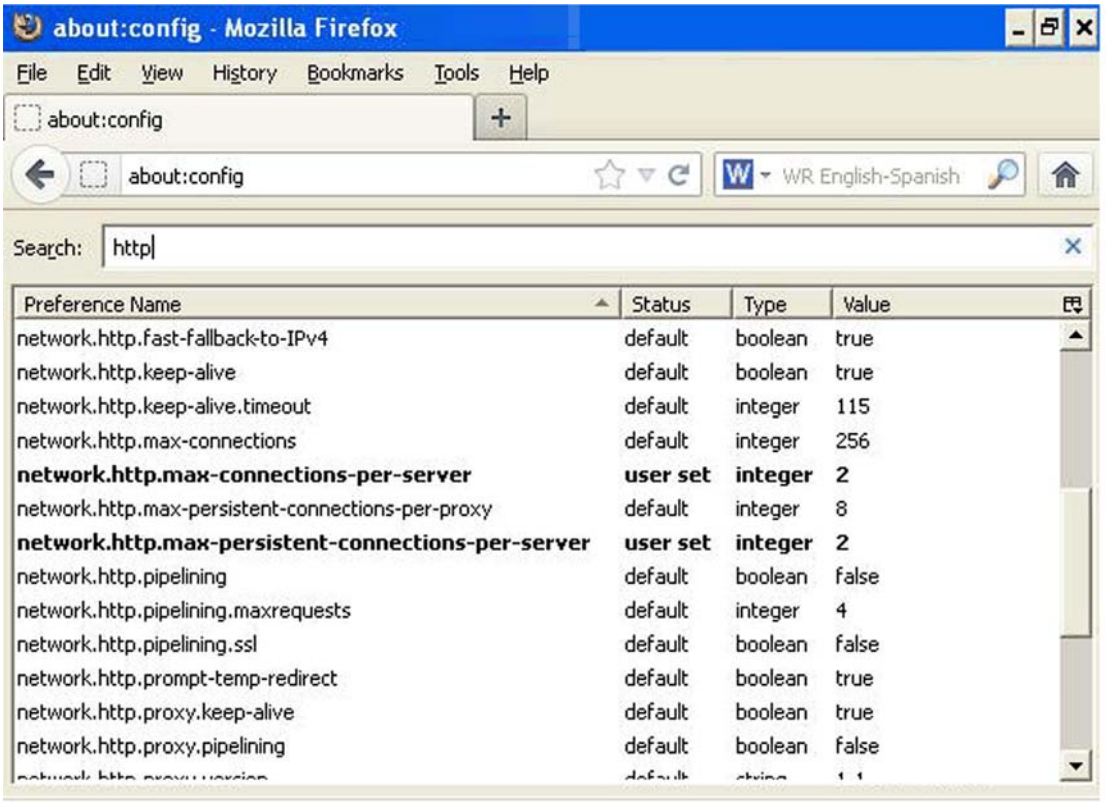
All data is presented as standard web pages in HTML format. To access web pages, use Internet Explorer 6.0 or 8.0 and Java 1.5 or greater.

This is the updated Windows registry entry when you use the TM168BACW and TM168MODW modules with Internet Explorer 8.0:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MAXCONNECTIONSPER1_0SERVER]
"explorer.exe"-dword: 00000004
"iexplore.exe"-dword: 00000004
```

This is the browser configuration when you use the TM168BACW and TM168MODW modules with Mozilla Firefox:


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
about:config
WR English-Spanish
Search: http
Preference Name Status Type Value
network.http.fast-fallback-to-IPv4 default boolean true
network.http.keep-alive default boolean true
network.http.keep-alive.timeout default integer 115
network.http.max-connections default integer 256
network.http.max-connections-per-server user set integer 2
network.http.max-persistent-connections-per-proxy default integer 8
network.http.max-persistent-connections-per-server user set integer 2
network.http.pipelining default boolean false
network.http.pipelining.maxrequests default integer 4
network.http.pipelining.ssl default boolean false
network.http.prompt-temp-redirect default boolean true
network.http.proxy.keep-alive default boolean true
network.http.proxy.pipelining default boolean false

Accessing the Embedded Web Pages

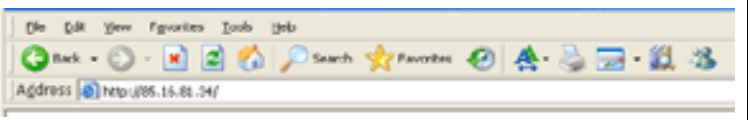
Initial Power-up

The TM168BACW and TM168MODW communication modules automatically install the embedded web pages for the controller the first time the module powers up after being inserted into the controller. During this initial installation (which can take several minutes) the web pages for the controller are not accessible. This delayed access of the web pages occurs only during the initial module power cycle, and does not occur on any subsequent power cycles or resets.

NOTE: Do not insert the communications module into a controller that is under power and has already been configured. If you do, the web pages for the controller are not accessible. Before you add the communication module, power down the controller. Then power up the controller with a communications module inserted. The communications module automatically installs the controller web pages at power-up.

Accessing the Embedded Web Pages

If you access the web pages for the controller after the initial power up, wait until the module status (**MS**) LED on the module stops alternately flashing red/green (or until a 'website loading' notice in the web page closes). Then you can attempt to access the web pages. Thereafter, use these steps to access the embedded web pages for the TM168BACW and TM168MODW communication modules:

Step	Action
1	Enter the IP address of the module in an Internet Explorer browser. 
2	This dialog box opens:

Step	Action
3	In the **Security** dialog box, type in these case-sensitive values and click **OK**: • **User name** • **Password** The **Home** page opens. **NOTE:** The **User name** is always USER. The default **Password** value is also USER, but can be changed in the Change Password web page. Change the default **Password** the first time you access the Web pages. For more security information, consult the instructions for changing the password *(see page 106)*.
4	In the **Home** page, select a language preference from the **Languages** list: • **English** (default) • **French** • **German** • **Italian** • **Spanish** The web page immediately displays its contents in the selected language.
5	To navigate to other parts of the embedded web site, open the appropriate link in the header or the menu bar.

Navigating the Embedded Web Pages (TM168BACW)

Introduction

This header area appears at the top of every TM168BACW web page:

The Web pages are a tool for reading and writing data, and control the state of the controller, with full access to all data in your application. If there are security concerns about these functions, assign a secure password to the Web pages.

For reasons of security for your installation, change the default password immediately upon the first login.

⚠ WARNING

UNAUTHORIZED DATA ACCESS

- Immediately change the default password to a new, secure password.
- Do not distribute the password to unauthorized or otherwise unqualified personnel.
- Disable the Web pages to prevent any unwanted or unauthorized access to data in your application.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: A secure password is one that has not been shared or distributed to any unauthorized personnel and does not contain any personal or otherwise obvious information. Further, a mix of upper and lower case letters, numbers and special characters offer the greatest security possible. You should choose a password length of at least 7 characters.

Refer to the instructions for changing a user password *(see page 106)*.

Links

Links in the header help you navigate through the embedded web pages:

Header Item	Corresponding Embedded Web Page
Home	Click **Home** to open the home page for the module, which includes these links: ● **Language:** Select a display language for the embedded web pages. ● **Identification** → **About:** View the current versions of the TM168BACW software components.
Documentation	This link opens the **Documentation** page, where you can access the Schneider Electric website for technical information and support.

Menu Bar Items

Links in the menu bar open embedded web pages for these functions:

Menubar Item	Corresponding Embedded Web Page
User Menu	For parametric controllers (chiller and air handling units), these menus contain the selections available on the **User Menu** and **Installation** menus on the HMI. Consult these HMI menus on the parametric controller for a description of their respective selections. These menus are not enabled for generic controllers.
Installation	

Maintenance	● **Ethernet Statistics**
	  ● global *(see page 117)*
	  ● port *(see page 118)*
	● **SNMP Statistics** *(see page 119)*
	● **Diagnostic Log** *(see page 120)*
	● **BACnet Statistics** *(see page 121)*
	● **BACnet Discovery** *(see page 122)*
	● **Diagnose BACnet** *(see page 123)*

Configuration	● **HTTP User Admin** *(see page 105)* ● **IP Configuration** *(see page 107)* ● **SNMP Agent** *(see page 110)* ● **BACnet** *(see page 113)* ● **Reboot** *(see page 112)*

Navigating the Embedded Web Pages (TM168MODW)

Introduction

These links appear at the top of every TM168MODW web page:

Links

Links in the header help you navigate through the embedded web pages:

Header Items	
Home	Click **Home** to open the home page for the module, which includes these links: ● **Language:** Select a display language for the embedded web pages. ● **Identification** → **About:** View the current versions of the TM168MODW software components.
Documentation	This link opens the **Documentation** page, where you can access the Schneider Electric website for technical information and support.
Menu Bar Links	
Monitoring	You can create and design custom web pages for your Modicon M168 connectivity module. *(see page 134)*
Control	The **Control** web page has a link to the **Reboot** page, where you can perform a warm reboot of the connectivity module *(see page 112)*.

Diagnostics	● Ethernet Statistics
	  ● Global *(see page 117)*
	  ● Port *(see page 118)*
	● SNMP Statistics *(see page 119)*
	● Diagnostic Log *(see page 120)*
	● Modbus Statistics
	  ● TCP Port *(see page 124)*
	  ● TCP Port Connections *(see page 125)*

Configuration	● Security
	  ● Password Change *(see page 99)*
	  ● User Administration *(see page 105)*
	● IP Parameters *(see page 107)*
	● SNMP Agent *(see page 110)*
	● Ethernet Ports *(see page 114)*
	● DNS Configuration *(see page 115)*

6.3 Configuring the Modicon M168 Ethernet Modules

Overview

Use the embedded web pages to configure the communication parameters for Modicon M168 Ethernet modules.

What Is in This Section?

This section contains the following topics:

Topic	Page
HTTP Account Administration	105
IP Parameter Configuration	107
SNMP Agent Configuration	110
Reboot Page	112
BACnet Network Parameter Configuration (TM168BACW)	113
Ethernet Port Configuration (TM168MODW)	114
DNS Configuration (TM168MODW)	115

HTTP Account Administration

Introduction

After you access the HTTP web pages for the TM168BACW or TM168MODW connectivity modules, you can perform these administrative actions:

- Add a new user.
- Delete a current user.
- Change a user password.

Dialog Box

Access the **User Accounts** dialog box from the home page for your module:

- TM168BACW: Go to the **Communication Module** → **HTTP User Admin.** link on the **Configuration** page.
- TM168MODW: Go to the **Security** link on the **Configuration** page.

The **User Accounts** dialog box appears:

Add a User

Create an account for a new user:

Step	Action
1	Enter a new (case-sensitive) user name in the **Name** field.
2	Enter a corresponding new (case-sensitive) password in the **Password** field.
3	Click the **Add** button to create the new account.

NOTE: There is a maximum of 10 user accounts at any time.

Change the User Password

Change the password for a user:

Step	Action
1	Enter the new (case-sensitive) password in the **New Password** field.
2	Enter the new password again in the **Confirm New Password** field.
3	Click the **Update** button.

Delete a User

Delete a user account:

Step	Action
1	Select the name of the user you want to delete in the **Users** list.
2	Click the **Delete** button to delete the new account.

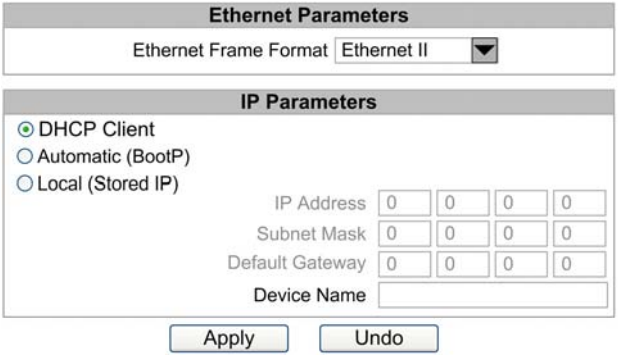
IP Parameter Configuration

Introduction

Access the IP parameters for the TM168BACW and TM168MODW connectivity modules on their **Configuration** web pages.

Introduction

Set the IP parameters for your module on this page:



You can configure these parameters:

- Select an Ethernet frame type.
- Specify the source of the IP addressing parameters of the module.
- Enter IP address settings (**Local (Stored IP)** only).
- Enter a **Device Name** (**DHCP Client** only).

Detailed descriptions of these parameters are below.

Selecting an Ethernet Frame Type

To specify an Ethernet frame type, select one of these values in the **Ethernet Frame Format** list:

- **Ethernet II**
- **IEEE 802.3**
- **Auto**: The device applies the appropriate format.

NOTE: A change made to the **Ethernet Frame Format** setting takes effect only after you reboot the module *(see page 112)*.

Specifying the Source of IP Address Settings

You can specify one of these sources for the IP address settings for the module from this list:

- **DHCP Client:** The module requests IP settings from a DHCP server located on the same subnet. Enter the **Device Name** of the module on this page so that it can be recognized by the DHCP server.
- **Automatic (BootP):** The module requests IP settings from a BootP server on the same subnet. The module identifies itself to the BootP server using its MAC address.
- **Local (Stored IP):** The module uses the **IP Address**, **Subnet Mask**, and **Default Gateway** settings input in this page.

NOTE: If the module does not receive an IP address from the selected source, it applies its default IP address *(see page 93)*.

Assigning a Stored IP Address

When you select **Local (Stored IP)**, you can enter IP address settings for the module. Access the embedded web pages *(see page 99)* and assign a stored IP address:

Step	Action
1	In the **IP Configuration** page, enter values for: ● **IP Address**: Enter 4-octet values (0...255) as a unique IP address. (Put the first octet in the range 1 ...126 or 128 ... 233.) ● **Subnet Mask**: Enter 4-octet values (0 ... 255). ● **Default Gateway** (optional): Enter 4-octet values (0...255) on the same subnet as the IP address. **NOTE:** Create a subnet mask configuration that matches the IP address class. For example, use the subnet mask 255.255.255.0 with a 4-octet (class C type) IP address such as 192.168.***x.y***.
2	Click one of these buttons: ● **Apply**: Save the edited IP addressing parameters. ● **Undo**: Clear the page without saving your edits.

NOTE: Changes made to the stored IP configuration take after effect you reboot the module with the **Reboot** Page or after a power cycle of the module.

Entering a Device Name

When you select **DHCP Client**, you can enter a **Device Name** for the module. Access the embedded web pages *(see page 99)* and enter a device name:

Step	Action
1	In the **IP Configuration** page, type in a **Device Name**. **NOTE:** The DHCP server uses this name as a unique identifier for the device, and assigns pre-determined IP address settings that are associated with this name.
2	Click one of these buttons: • **Apply**: Save the edited IP addressing parameters. • **Undo**: Clear the page without saving your edits.

SNMP Agent Configuration

Introduction

The TM168BACW and TM168MODW connectivity modules have SNMP agents that connect to and communicate with an SNMP manager through the UDP transport protocol over ports 161 and 162.

The SNMP service includes:

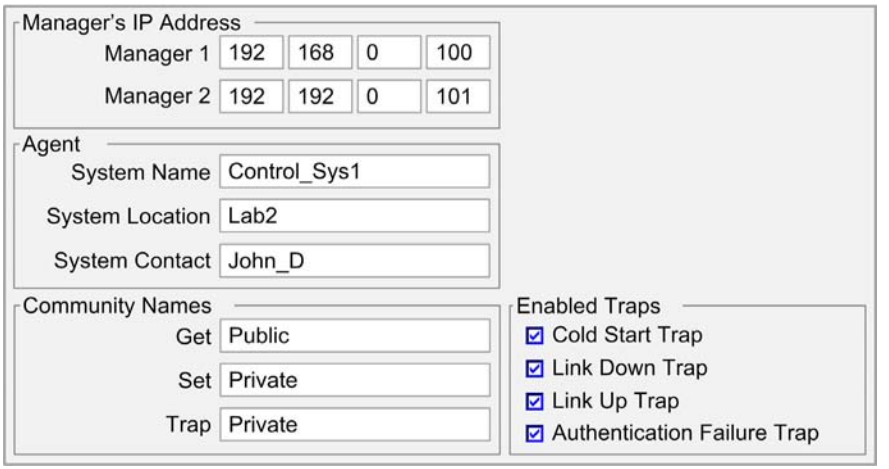
- An SNMP manager can automatically discover and identify the module.
- The module can authenticate an SNMP manager that sends requests to the module.
- SNMP can manage events (or traps) that the module reports, including the identification of 2 SNMP managers that are authorized to receive reports.

Web Page

Access the SNMP agent for the TM168BACW and TM168MODW connectivity modules:

- TM168BACW: Access the SNMP agent from the **Setup** web page.
- TM168MODW: Access the SNMP agent from the **Configuration** web page.

This figure shows the configurable parameters for the SNMP agent:



Parameter Descriptions

Manager IP Address parameters:

Manager 1	These fields contain the IP address of the first (**Manager 1**) and second (**Manager 2**) SNMP manager (consists of 4-octet decimal values, 0...255). Put the first octet value of each SNMP manager IP address in the range 1...126 or 128...223.
Manager 2	

Agent parameters:

System Name	This user-defined string describes the controller.
System Location	This string describes the location of the controller.
System Contact	This string identifies the contact person for the controller.

Community Name parameters:

Get	Enter the passwords for the parameters **Get**, **Set**, and **Trap**. (They can be empty.) The maximum password length is 16 printable ASCII characters. The default setting for each community name is `public`.
Set	
Trap	

Enabled Trap parameters:

Cold Start Trap	The agent is reinitializing. Its configuration may be altered.
Link Down Trap	One of the communication links for the agent has turned off.
Link Up Trap	One of the communication links for the agent has turned on.
Authentication Failure Trap	The agent received a request from an unauthorized manager.

Finish the Configuration

After you configure the parameters, click a button:

- **OK:** Save and apply changes.
- **Cancel:** Cancel or undo changes.

Reboot Page

Introduction

Use the reboot operation to perform a warm reboot of the TM168BACW or TM168MODW connectivity module:

- TM168BACW: Access the reboot function on the **Configuration** web page.
- TM168MODW: Access the reboot function on the **Control** web page.

Reboot Button

The reboot button activates any pending configuration changes (such as an edited IP address) made to the module via the web pages. During the reboot operation, the connectivity module is offline.

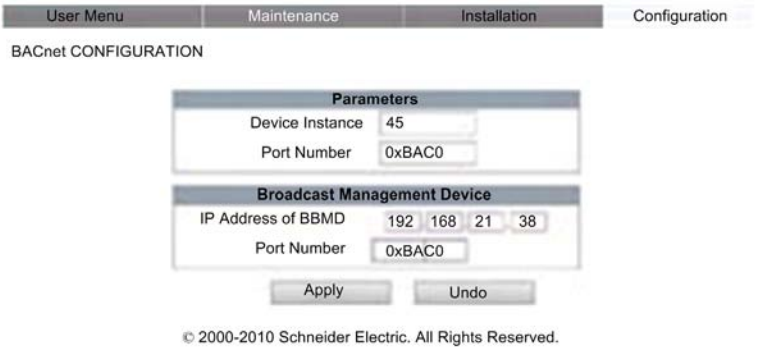
Click **Reboot** to cause the TM168BACW or TM168MODW module to become non-operational temporarily during the reboot process:

Performing a reboot in this web page does not reboot the controller. The controller continues to run during the reboot operation.

BACnet Network Parameter Configuration (TM168BACW)

Introduction

Use the **BACnet Configuration** page to configure BACnet communications. To access the **BACnet Configuration** page, click the **Configuration** menu and select **Communication Module → BACnet**:



NOTE: The BACnet MAC ID is constructed using the module **IP Address** configured in the IP Configuration web page *(see page 107)* and the **Port Number** configured in this page.

Parameters

The **BACnet Configuration** screen presents these parameters and controls:

Parameters area:	
Device Instance	This number is the network identifier of the device (or the device ID). It identifies the device on the BACnet network. Us a number that is unique with respect to all devices on the BACnet network.
Port Number	The port the device will be listening on. The default BACnet port is 47808 (or BAC0 in hexadecimal).
Broadcast Management Device area:	
IP Address of BBMD	The BACnet Broadcast Management Device (BBMD) IP address, typically a private address range—for example, an IPv4 address beginning with the octets 192.168. **NOTE:** Local and foreign BACnet devices both use this address to register with the BBMD to be able to send and receive local BACnet communications.
Port Number	The port the device will be broadcasting on. The default BACnet port is 47808 (or BAC0 in hexadecimal).
Controls:	
Apply	Click this to save the changes you have made to this page.
Undo	Click this to clear the changes you have made without applying them, and revert to the prior settings.

Ethernet Port Configuration (TM168MODW)

Introduction

This topic describes the Ethernet port configuration for the TM168MODW module.

Web Page

Access the Ethernet port configuration parameters from the **Configuration** web page:

Parameters

Parameter	Description	
Port Number	Choose the port number to configure.	
Port Control	Speed	Displays the current link speed in Mbps (10 or 100).
	Duplex Mode	A display of the current duplex mode (full/half).
	Auto Negotiation	Select the state of auto negotiation (enabled/disabled).

Finish the configuration:

- **Apply** (save)
- **Undo** (cancel)

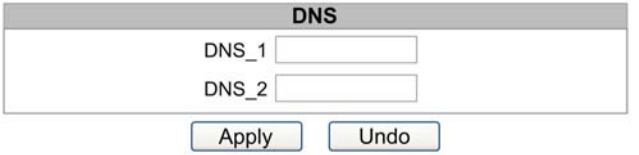
DNS Configuration (TM168MODW)

Introduction to DNS

The DNS (Domain Name System) is a distributed database that stores and associates many types of information with domain names and translates domain names (computer hostnames) to IP addresses. DNS is mandatory for sending email. Configure the DNS service in order to reach devices over the Internet by its name.

You can access the **DNS Configuration** web page via the **Configuration** menu on the TM168MODW home page *(see page 103)*.

DNS Configuration Web Page



DNS_1 and **DNS_2** are the alpha-numeric domain names that represent the servers from which IP parameters are obtained.

6.4 Monitoring and Diagnosing the Status of the Modicon M168 Ethernet Module

Introduction

This section describes web pages that allow you to view the status and diagnose your Modicon M168 connectivity module.

What Is in This Section?

This section contains the following topics:

Topic	Page
Global Ethernet TCP/IP Statistics	117
Ethernet Port Statistics	118
SNMP Statistics	119
Diagnostic Log	120
BACnet Statistics (TM168BACW)	121
BACnet Discovery (TM168BACW)	122
Diagnosing BACnet (TM168BACW)	123
Modbus TCP Port Statistics (TM168MODW)	124
Modbus TCP Port Connections Statistics (TM168MODW)	125
Monitoring (TM168MODW)	126

Global Ethernet TCP/IP Statistics

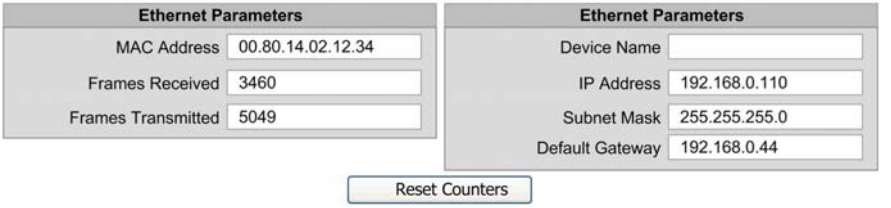
Introduction

You can view global Ethernet statistics for the TM168BACW and TM168MODW connectivity modules:

- TM168BACW: Use the **Communication Module** → **Ethernet Statistics** → **Global** link on the **Maintenance** web page.
- TM168MODW: Use the **Ethernet Statistics** → **Global** link on the **Diagnostics** web page.

Web Page

The web page shows these Ethernet statistics:



Parameter descriptions:

Parameter		Description
Ethernet Parameters	MAC Address	the global Ethernet MAC address of the module (assigned at the factory)
	Frames Received	the number of Ethernet frames successfully received on each Ethernet port on the module
	Frames Transmitted	the number of Ethernet frames successfully transmitted by both Ethernet ports on the module
TCP/IP Parameters	Device Name	the device name of the module
	IP Address	IP addressing parameters
	Subnet Mask	
	Default Gateway	

NOTE: The counting statistics on this page are automatically refreshed. You can also click the **Reset Counters** button to reset the **Frames Received** and **Frames Transmitted** counting statistics to 0.

Ethernet Port Statistics

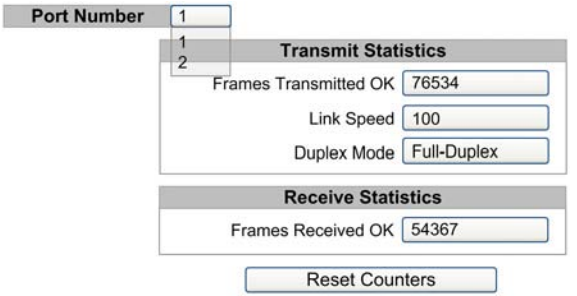
Introduction

You can view Ethernet port statistics for the TM168BACW and TM168MODW connectivity modules:

- TM168BACW: Use the **Communication Module** → **Ethernet Statistics** → **Port** link on the **Maintenance** web page.
- TM168MODW: Use the **Ethernet Statistics** → **Port** link on the **Diagnostics** web page.

Introduction

Use this page to view statistical information related to the Ethernet ports. The counting statistics on this page are automatically refreshed:



NOTE: The **Receive Statistics** field applies only to the TM168BACW module.

The page contains these data fields:

- **Port Number**: Select a port (1, 2) to display its statistics.
- **Transmit Statistics**
  - **Frames Transmitted OK**: This field contains the number of successfully transmitted frames.
  - **Link Speed**: This is the current speed of the link in Mbps (10 or 100).
  - **Duplex Mode**: This reports the current duplex mode (full/half).
- **Receive Statistics** (TM168BACW)
  - **Frames Received OK**: This is the number of successfully received frames.

Click **Reset Counters** to reset all counting statistics.

SNMP Statistics

Introduction

You can view SNMP statistics for the TM168BACW and TM168MODW connectivity modules:

- TM168BACW: Use the **Communication Module** → **SNMP Statistics** → **Port** link on the **Maintenance** web page.
- TM168MODW: Use the **Ethernet Statistics** → **Port** link on the **Diagnostics** web page.

Web Page

The web page looks like this:

Parameter descriptions:

- **SNMP Agent Status** is operational or idle.
- **Invalid Community Names** counts the requests sent to the module that contain invalid community names that indicate that the requesting device may be unauthorized to make such a request.
- **Received Messages** counts the number of SNMP requests received by the module.
- **Transmitted Messages** counts the number of SNMP responses sent by the module.

Click **Reset Counters** to reset these counting statistics.

Diagnostic Log

Introduction

The **Diagnostic Log** contains information that is collected during operations. You can view the diagnostic logs for the TM168BACW and TM168MODW connectivity modules:

- TM168BACW: Use the **Communication Module** → **Diagnostic Log** link on the **Diagnostics** web page.
- TM168MODW: Use the **Diagnostic Log** link on the **Diagnostics** web page.

The Web Page

This is a sample diagnostic page:

Options:

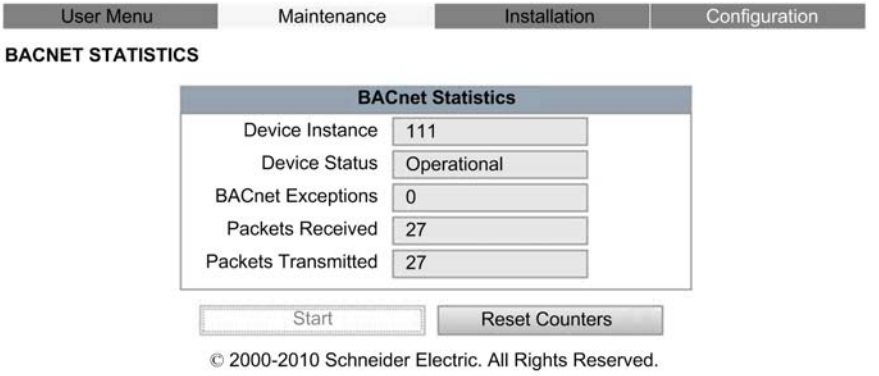
- Click **Reload** to update the display. (This page is not automatically updated.)
- Click **Clear** to clear the log. Deleting the log removes its content from flash memory.
- Click **Save to File** (above the message) to save the current contents of the **Log File** in a new Notepad file.

BACnet Statistics (TM168BACW)

Introduction

Use the **BACnet Statistics** page to view status and packet information for the TM168BACW module. This page is automatically updated every 3 seconds.

To view this page, open the **Maintenance** menu and select **Communication Module → BACnet Statistics**.



Parameters

The **BACnet Statistics** page contains these parameters and controls:

Parameters:	
Device Instance	The numerical identifier for the device on the network.
Device Status	The operating status of the device: • Operational • Operational, Read Only • Download Required • Download in Progress • Non-Operational
BACnet Exceptions	This is the number of packets that were not successfully transferred to the device.
Packets Received	This is the number of packets that were sent by another source and received by the device.
Packets Transmitted	This is the number of packets sent by the device.
Controls:	
Start	Click **Start** to begin the display of device data.
Reset Counters	Click **Reset Counters** to set the counting parameters (BACnet Exceptions, Packets Received, and Packets Transmitted) to 0.

BACnet Discovery (TM168BACW)

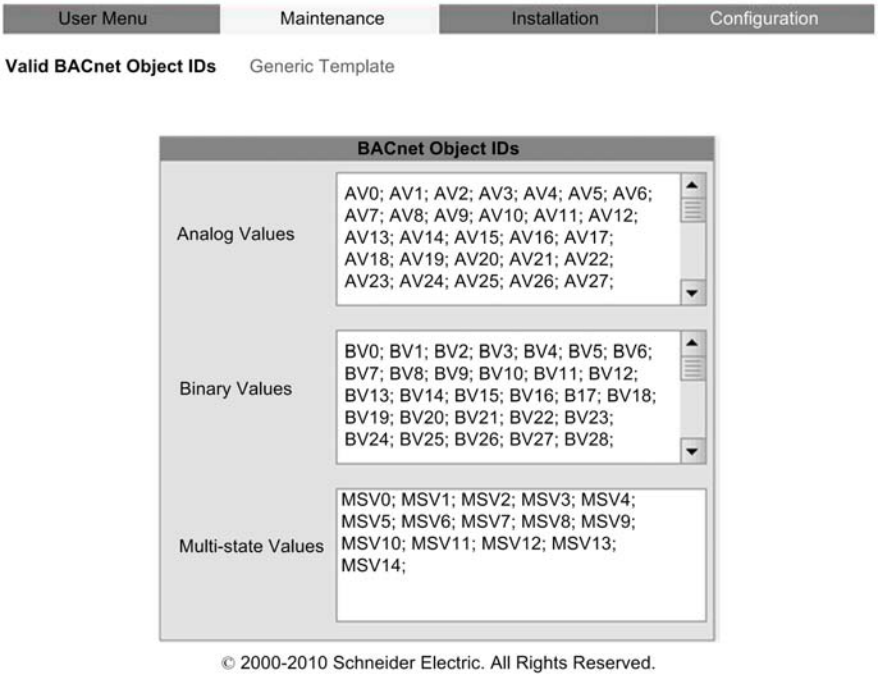
Introduction

Use the **BACnet Discovery** page to view the BACnet object IDs for the analog, binary, and multi-state values.

To view the page, open the Maintenance tab *(see page 102)* and select the **BACnet Discovery** link.

Dialog Box

This example of the **BACnet Object IDs** dialog window shows valid BACnet object IDs for analog, binary, and multi-state values:

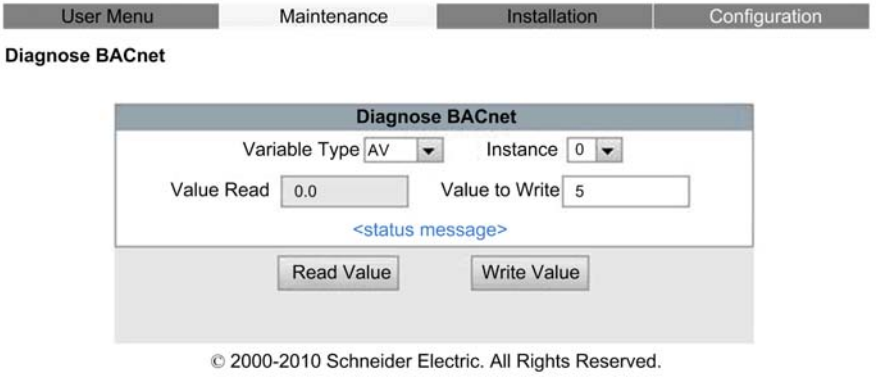


Diagnosing BACnet (TM168BACW)

Introduction

Use the **Diagnose BACnet** page to troubleshoot a BACnet client. You can read and write to the first 10 analog values, binary values, and multi-state values of your device.

To view this page, open the **Maintenance** menu and select **Communication Module** → **Diagnose BACnet**.



Parameters

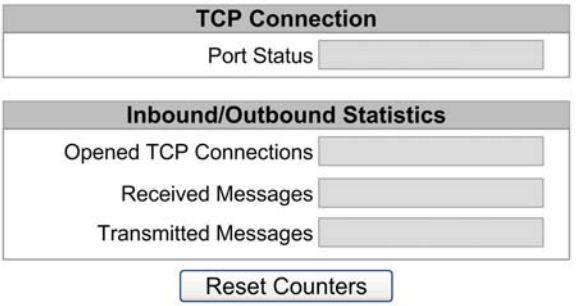
The **Diagnose BACnet** page contains these parameters and controls:

Parameters:	
Variable Type	This parameter identifies the type of variable: • AV (analog value) • BV (binary value) • MSV (multi-state value)
Instance	This is the object instance identifier of the AV, BV, or MSV object you will read or write to.
Value Read	This is the value of the selected variable type and instance. It is read from the device when you click **Read Value**.
Value to Write	This is the value that is written to the specified variable type and instance when you click **Write Value**. (Use only positive integers or floating point numbers in this field.)
<Status Message>	This is the result of the most recent write-value event.
Controls:	
Read Value	Click **Read Value** this to read the value of the specified variable type and instance.
Write Value	Click **Write Value** to write the input value to the specified variable type and instance.

Modbus TCP Port Statistics (TM168MODW)

Web Page

Click the **Modbus Statistics** → **TCP Port** link on the **Diagnostics** page to see the Modbus TCP port statistics for the TM168MODW connectivity module:



Parameters

Modbus TCP parameters:

Parameter		Description
TCP Connection	Port Status	This is the status of the port.
Inbound/Outbound Statistics	Opened TCP Connections	This is the number of Modbus clients currently connected.
	Received Messages	This is the total number of Modbus requests.
	Transmitted Messages	This is the total number of Modbus responses.

Click **Reset Counters** to set the counting parameters to 0.

Modbus TCP Port Connections Statistics (TM168MODW)

Introduction

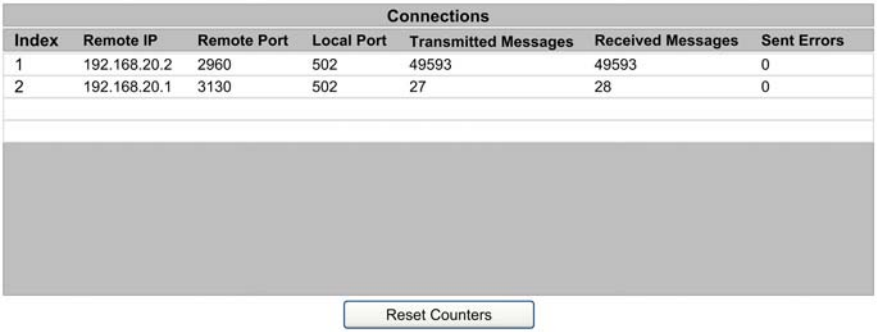
Use the TCP port connections web page to display a list of open TCP connections for the TM168MODW connectivity module.

Click the **Reset Counters** button on this page to clear the counting statistics.

NOTE: This page is automatically updated. The counting statistics are automatically cleared when the module is powered-up or reset.

Web Page

Access this page with the **Modbus Statistics** → **TCP Port Connections** link on the TM168MODW **Diagnostics** page:



Parameter Descriptions

TCP port connection diagnostic data:

Column	Description
Index	The connection sequence number.
Remote IP	The IP address of the connected remote device.
Remote Port	The port number of the connected remote device used to make the connection.
Local Port	The port number of theM340 EGD used to make the connection.
Transmitted Messages	A count of the number of Modbus messages sent over this connection.
Received Messages	A count of the number of Modbus messages received on this connection.
Sent Errors	A count of the number of Modbus TCP sent errors detected over this connection.

Monitoring (TM168MODW)

Introduction

You can view the user-configured Modbus information for the TM168MODW module on the **Monitoring** page.

Web Page

To view the **Modbus Generic** screen, use the **Monitoring** → **Custom Page** on the **Monitoring** page for the TM168MODW module:

Modbus Generic			
Name	ID	Value	
AV2	4	0	Write
AV2	4	0	Write
AnalogValue1	3	0	Write
AV2	4	0	Write
MyAnalog4	5	0	Write
MyAnalog5	6	0	Write
MyAnalog6	7	0	Write
MyAnalog7	8	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write
MyAnalog8	9	0	Write

NOTE: This page monitors the user-configured information in the file `wwwroot/html/monitoring/secure` *(see page 128)*. There is a maximum of 20 parameters.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not create a web page that allows remote write access to critical application parameters unless you have performed a thorough analysis of the implications of unintended remote access.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

6.5 Customizing Modicon M168 Connectivity Module Web Pages

Overview

This section contains instructions for customizing and personalizing the web pages associated with your device. You must have a working familiarity with these topics:

- File Transfer Protocol (FTP) communications (through the Windows command line interface or FTP client software)
- Basic web page hyper-text mark-up language (HTML) knowledge (including commonly used HTML mark-up tags and hexadecimal color codes)

You can verify communications with a specific controller by looking at the MAC address printed on the front of the TM168BACW or TM168MODW module and comparing it to the MAC address on the global diagnostics web page.

For critical applications, consider using a Modicon M168 controller output that is wired to a visual indicator that indicates communications with a specific Modicon M168 controller.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Always verify that you are connected to the correct Modicon M168 controller by verifying the MAC address of that controller.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

What Is in This Section?

This section contains the following topics:

Topic	Page
Accessing the Web Configuration File	129
Editing the Web Configuration File	132

Accessing the Web Configuration File

Introduction

Edit the web page configuration file `config.js` to change the web page design:

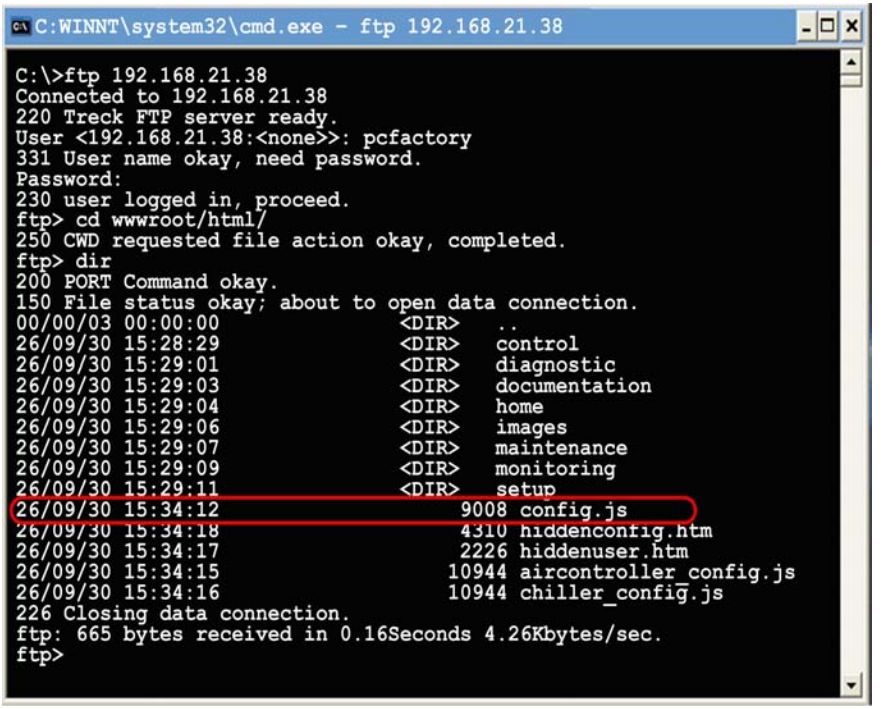
Stage	Description
1	Download the configuration file from the device to your PC.
2	Using a text editor of your choice, edit the contents of the configuration file.
3	Upload the edited configuration file from your PC to the device.

Downloading the Web Configuration File

To edit the web configuration file of the device, locate the file:

Step	Action
1	Open an FTP session with the Modicon M168 connectivity module. For example, if the IP address of the module is 192.168.21.38 type this text at the command prompt: `ftp 192.168.21.38.`
2	When prompted, type the user name and hit `Enter`. The default user name is `pcfactory`.
3	When prompted, type the password and hit `Enter`. The default password is also `pcfactory`.
4	Navigate to the directory that contains the configuration file (wwwroot/html). At the command prompt type: `ftp> cd wwwroot/html/` and hit `Enter`.

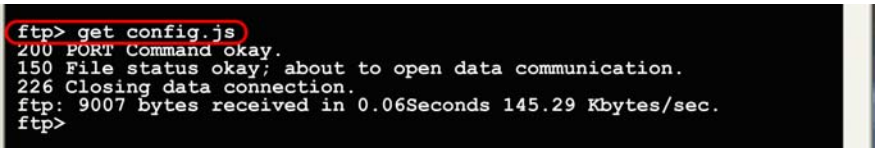
This window shows the above series of commands and the FTP responses:



Download the file you located above:

Step	Action
5	Download the configuration file with a `get` operation. At the command prompt type `ftp> get config.js` and hit `Enter`. **NOTE:** The file will download to the current PC directory from which you opened the command line interface. In this case, the C:\ directory.

This command and the FTP response looks like this:



NOTE: The file will download to the current PC directory from which you opened the command line interface. In this case, it is in the C:\ directory.

Changing the Web Configuration File

You can change these characteristics of the configuration file (`config.js`):

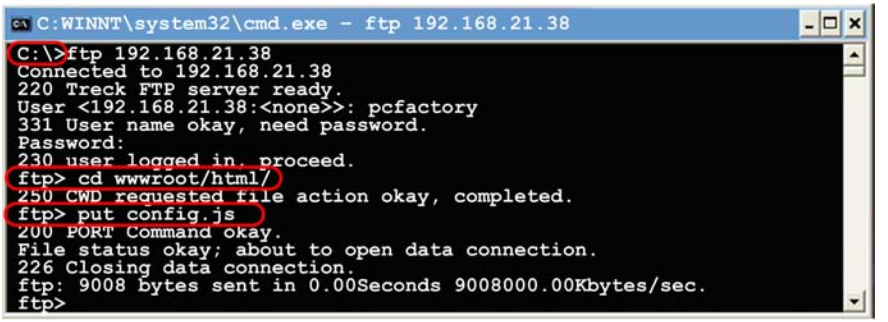
- Change the colors *(see page 132)* of the title bar and the title.
- Change the web page logo *(see page 133)*.
- Create custom pages *(see page 134)* for monitoring the device.

Uploading the Edited Web Configuration File

After you make changes to the `config.js` configuration file, upload the edited file from your PC to the device:

Step	Action
1	Open a session with the Modicon M168 connectivity module. **NOTE:** Open the FTP session from the directory on your PC where the configuration file is located (For example: `C:\`).
2	When prompted, type the user name and hit `Enter`. (The default user name is `pcfactory`.)
3	When prompted, type the password and hit `Enter`. (This default password is also `pcfactory`.)
4	Navigate to the directory that contains the configuration file (wwwroot/html). At the command prompt type `ftp> cd wwwroot/html/` and click `Enter`.
5	At the command prompt type `ftp put config.js` and click `Enter`.

This is the command and the FTP response:



Editing the Web Configuration File

Introduction

After you have downloaded the web configuration file from the device to your PC *(see page 129)*, you can edit its contents:

- Change the colors of the web page title bar and title.
- Change the web page logo.
- Create custom pages for monitoring the device.

Changing the Color of the Title Bar and Title

Change the colors of the web page title bar and title:

Step	Action
1	Using the text editor of your choice, open the web configuration file `config.js`. At the top of the file, this text (or similar text) is displayed:
2	Edit these parameters: • `TitleBGColor`: Assign a background color to the title bar. • `TitleColor`: Assign a color to the letters in the title. (You can use HTML hexadecimal color values or HTML color names.) The values used in the file above produce white text on a green background:
3	Save your edits in the text editor.
4	Upload the edited configuration file *(see page 131)* from your PC to the device.

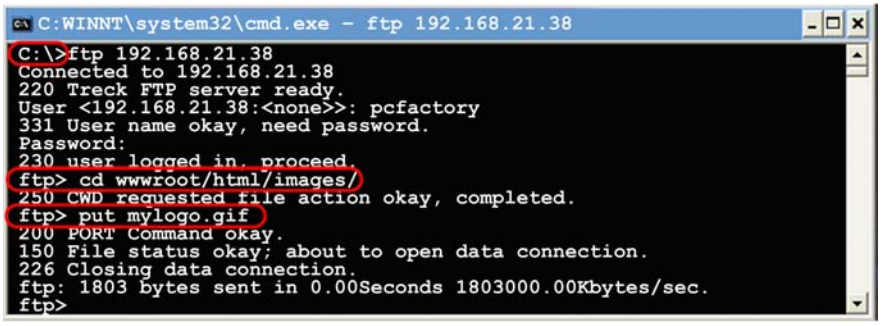
Changing the Logo

You can edit the web page logo by substituting your choice of graphic image for the Schneider Electric.gif graphic. Use an image in the .GIF format with a maximum size of 304 pixels wide by 55 pixels high.

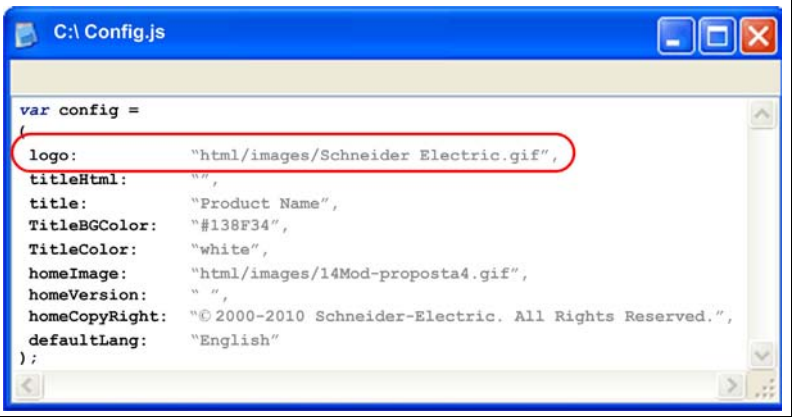
Upload the new graphic (for example, `mylogo.gif`) through FTP to the `wwwroot/html/images` directory of your device:

Step	Action
1	Open an FTP session with the Modicon M168 connectivity module. **NOTE:** Open the FTP session from the directory on your PC where the new graphic image file is located (for example: `C:\`).
2	When prompted, type the user name and click `Enter`. (The default user name is `pcfactory`.)
3	When prompted, type the password and click `Enter`. (The default password is also `pcfactory`.)
4	Navigate to the directory that contains the configuration file (wwwroot/html/images). At the command prompt type: `ftp> cd wwwroot/html/images/` and hit `Enter`.
5	At the command prompt, type `ftp put mylogo.gif` and click `Enter`.

This window shows the command and the FTP response:



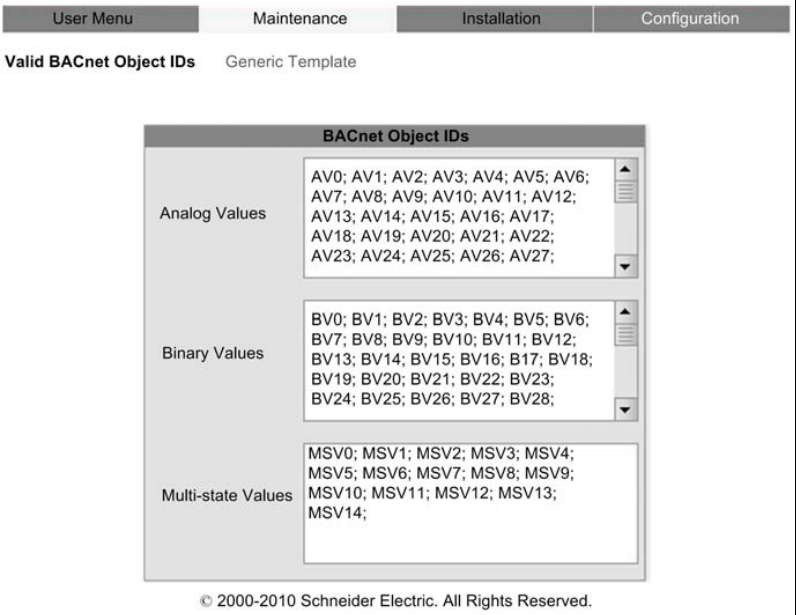
Change the name of the logo graphic in the configuration file:

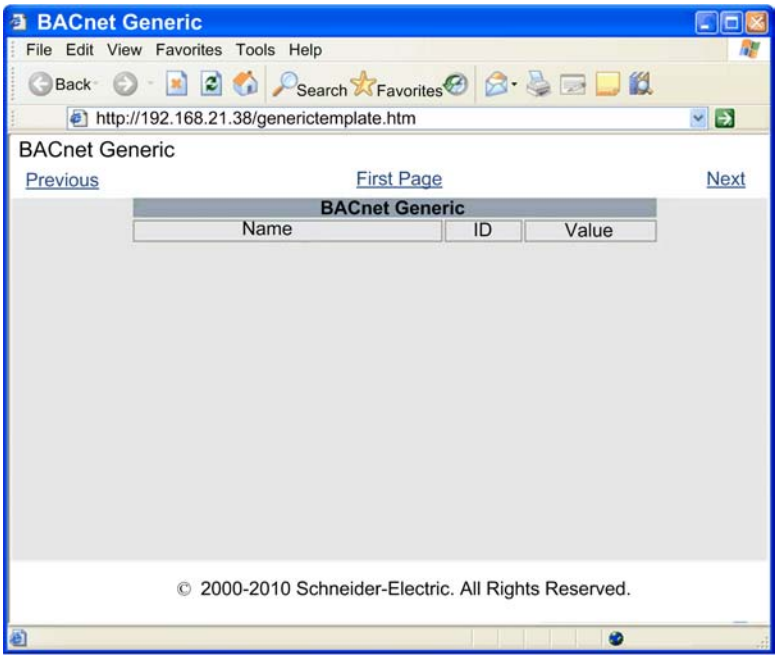
Step	Action
6	Using the text editor of your choice, open the web configuration file `config.js`. At the top of the file, this text (or text very much like it) is displayed: 
7	Edit these parameters: • `TitleBGColor`: Edit the background color of the title bar. • `TitleColor`: Edit the color of the letters in the title. To edit the graphic, change the `logo` parameter to the new graphic name (in this case `mylogo.gif`). The new example logo looks like this:
8	Save your edits in the text editor.
9	Upload the edited configuration file *(see page 131)* from your PC to the device.

Creating Custom Web Pages for Monitoring BMS Parameters

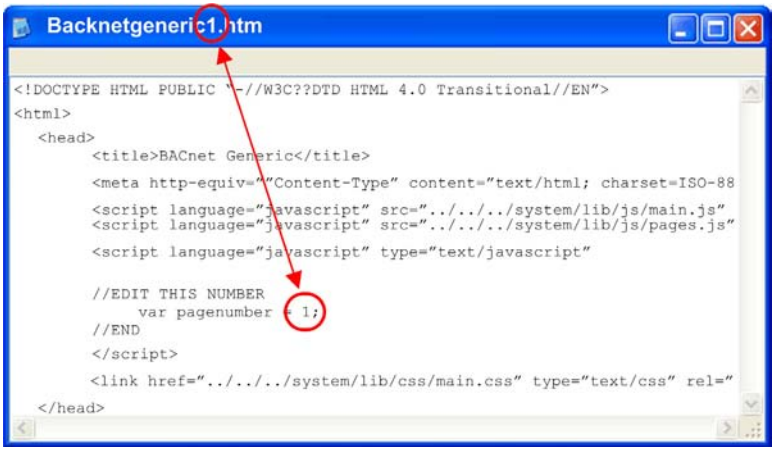
You can create and design custom web pages for your Modicon M168 connectivity module. Each custom web page displays only the device parameters you select. You can build pages to meet your particular device monitoring requirements. Customized web pages are created one at a time.

Connect to the device via HTTP and save a customizable web page to your PC:

Step	Action
1	Open an Internet browser and type in the target device IP address to connect to the embedded web pages of the device. (In this example, the IP address of the device is 192.168.21.38.)
2	In the device web pages, open the **Maintenance** menu and select **BACnet Discovery**. A web page opens. It displays a list of BACnet Object IDs and a menu that includes the **Generic Template** command:  **NOTE:** Later, you will refer to the list of BACnet objects to identify the objects you want to add to your custom web page.

Step	Action
3	Click the **Generic Template** command (above) to open a generic web page: 
4	With the **BACnet Generic** page open in your Internet browser, select **View** → **Source**. The contents of the BACnet generic page are displayed in a text file with an .HTM extension.
5	Before you edit the **BACnet Generic** page, save this page to your PC (**File** → **Save As**). **NOTE:** Name the new file `bacnetgenericN.htm`, where ***N*** is the sequence number of the customized web page: ● If this is your first customized web page, name it `bacnetgeneric.htm` with no numeric designation. (Web page numbering is zero based.) ● If this is your second customized web page, name it `bacnetgeneric1.htm`

Edit the contents of the new custom web page. Specifically, change the page number and add a list of BACnet objects to the page:

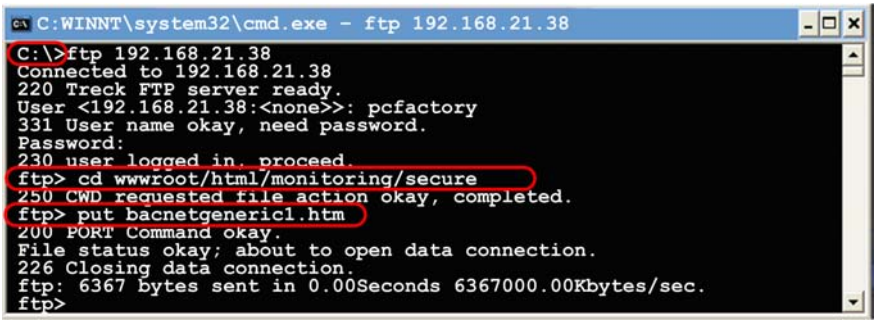
Step	Action
6	In the generic web page (which is still open on your PC), look for “EDIT THIS NUMBER.” On the next line (after the text `var page number =`), change the integer value to equal the page number for the new web page. **NOTE:** This number must be the same number that appears in the name of the generic file name. For example, if the web page name is `bacnetgeneric1.htm`, the `var page number` value must be 1: 
7	In the generic web page, navigate to the text that reads: `/* READ ME FIRST`.
8	Read the comments that follow `/* READ ME FIRST`.
9	In the lines that follow the comments, you can enter up to 20 BACnet object values. To enter a value, type the BACnet object name between the 2 adjacent quotation marks. For example, to include the analog value AV0, begin with the first following line and type: `document.writein('<param name>="id0" value="AV0" />');` **NOTE:** Refer to the **BACnet Discovery** page (see step 2, above) for a list of available BACnet object values.
10	Save your edits to this file.

Upload the new custom web page with FTP to the `wwwroot/html/monitoring/secure` directory of your device:

Step	Action
11	Open an FTP session with the Modicon M168 connectivity module. **NOTE:** Open the FTP session from the directory on your PC where the new web page HTML file is located (for example: `C:\`).

Step	Action
12	When prompted, type the user name and click `Enter`. (The default user name is `pcfactory`.)
13	When prompted, type the password and click `Enter`. (The default password is also `pcfactory`.)
14	Navigate to the directory to which you will transfer the new web page graphic: wwwroot/html/monitoring/secure: **a.** Type this at the command prompt: `ftp> cd wwwroot/html/monitoring/secure/` **b.** Click `Enter`.
15	Transfer the new graphic to the device: **a.** Type this at the command prompt: `ftp put bacnetgeneric1.htm` **b.** Click `Enter`. **NOTE:** Include the file name (`bacnetgenericN.htm`) in your `put` command. (The file name `bacnetgeneric1.htm` is only an example.)

This window shows the command and the FTP response:



Application Example

7

7.1 BACnet Application Example

What Is in This Section?

This section contains the following topics:

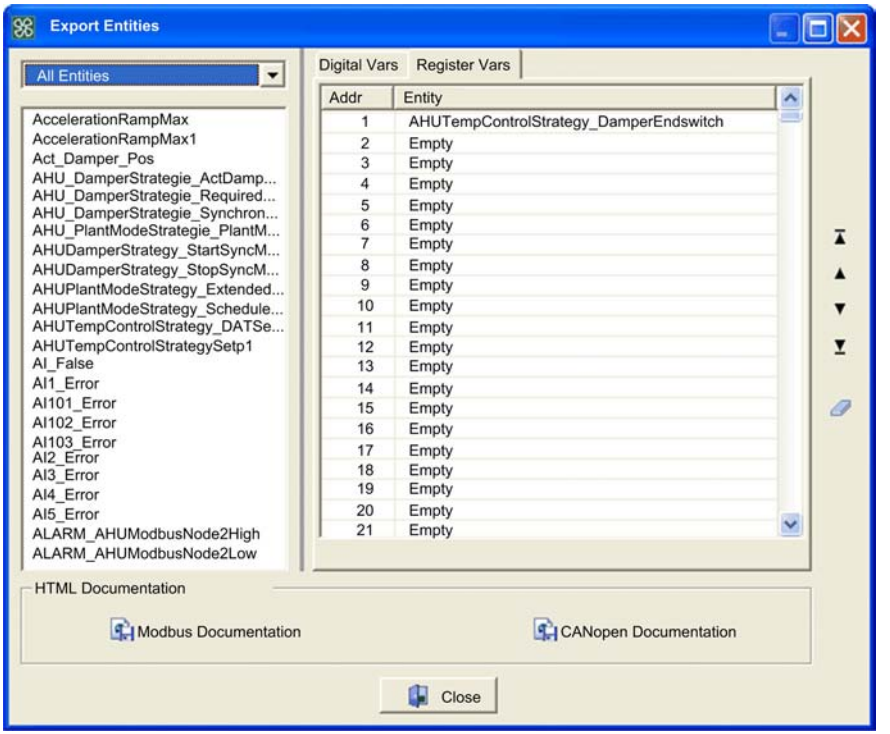
Topic	Page
Exporting Entities and Generating a BACnet Profile	140
Editing the BACnet Profile	142

Exporting Entities and Generating a BACnet Profile

Introduction

Export entities using the SoHVAC software after you have configured BACnet communication *(see page 69)* for the TM168BACS module or selected the controller and module *(see page 74)* for the TM168BACW module.

Open the **Export Entities** dialog box (**Tools** → **Export Entities**):



⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not export critical application parameters that would result in remote write access unless you have performed a thorough analysis of the implications of unintended remote access.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Export Entities

Follow these steps:

Step	Action
1	Move the desired entities to the right pane and click **Close**. (The profile does not generate unless you export a clock function block.)
2	Save your project (**File** → **Save Project**).
3	Generate the BACnet profile (**Tools** → **BMS Configuration** → **Generate BACnet profile**). **NOTE:** If you do not export at least one entity to generate the BACnet profile, this dialog box opens: Click **OK** to close this dialog box.
4	This dialog box indicates that the BACnet profile was successfully generated. Click **OK**.

Editing the BACnet Profile

Before You Begin

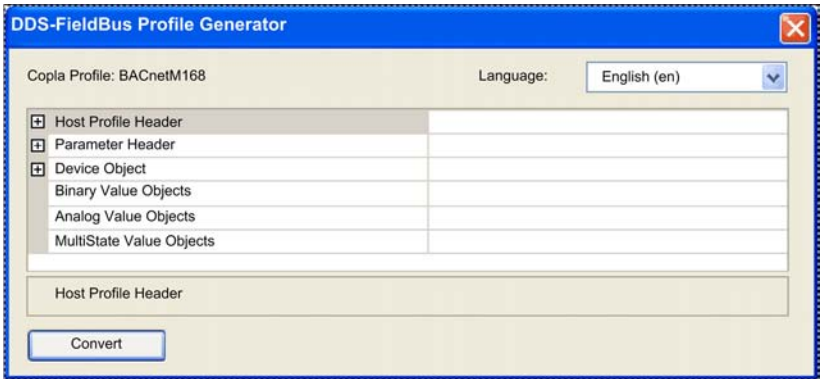
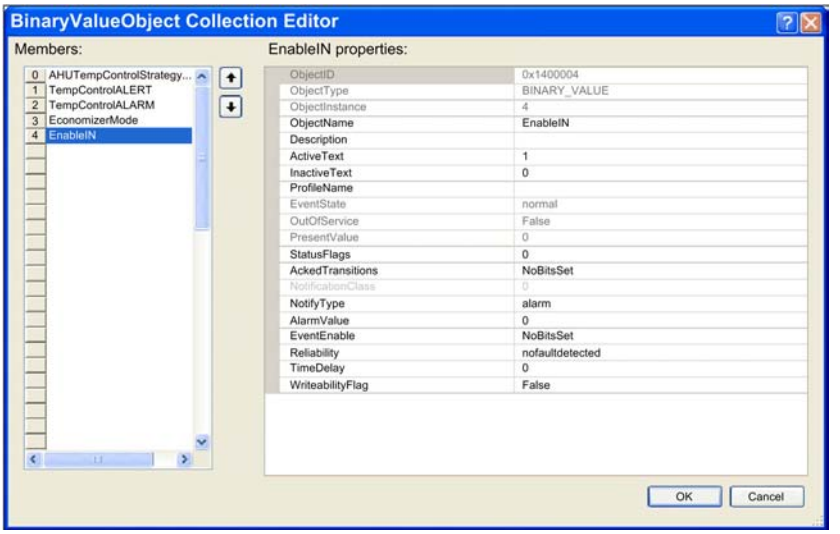
You can edit the BACnet profile only when your application is configured for BACnet MS/TP communications. If your application is designed to use the BACnet IP protocol, temporarily configure your application to use BACnet MS/TP communications. After editing the BACnet profile, you can reconfigure your application for BACnet IP communications.

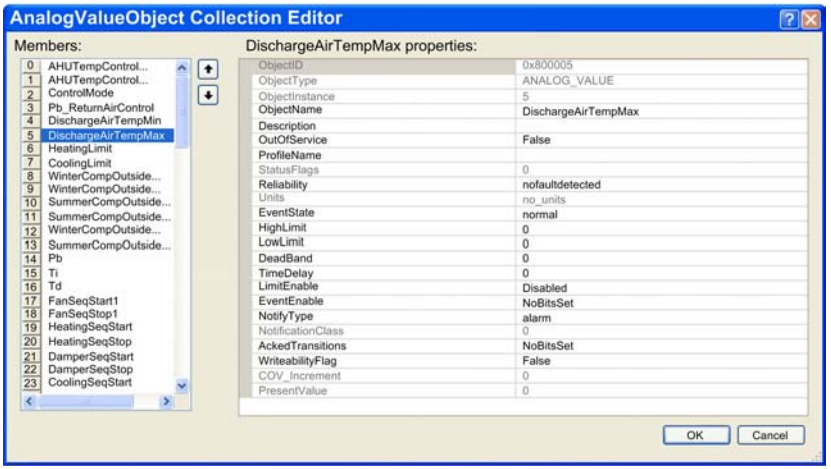
Configure a BACnet IP project for temporary BACnet MS/TP communications:

Step	Action
1	With your BACnet IP project open, select **Project** → **Hardware Expert...** to start the hardware configuration wizard.
2	Click **Next** to advance to step **2. Controller**.
3	Select a controller with a connectivity slot (indicated by the suffix “C”).
4	Click **Next** to advance to step **3. Serial Ports**.
5	For the **NETWORK CONNECTIVITY SLOT**, select **BACnet MS/TP**.
6	Click **Next** until you advance to the **Goodbye** page.
7	Click **End**.
8	Use the steps in the next section (*Editing the BACnet Profile*) to complete your BACnet profile edits.
9	After you edit the BACnet profile, use the **Hardware Expert**: ● Select the BACnet IP controller you are using (step 2 of the wizard). ● Configure the **NETWORK CONNECTIVITY SLOT** for **BACnet IP** communications (step 3 of the wizard).

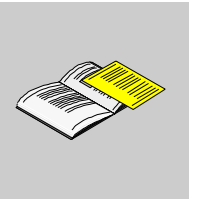
Editing the BACnet Profile

Edit the BACnet profile with the SoHVAC software:

Step	Action
1	Open the BACnet file editor (**Tools** → **BMS Configuration** → **Edit BACnet profile**). The **DDS-FieldBus Profile Generator** window opens. 
2	Select **Binary Value Objects** and click the ellipsis to open the **BinaryValueObject Collection Editor**: 
3	Select a member and edit the editable values. Click **OK** to accept your changes and return to the **DDS-FieldBus Profile Generator** window.

Step	Action
4	Select **Analog Value Objects** and click the ellipsis to open the **AnalogValueObjects Collection Editor**: 
5	Select a member and edit the values. Click **OK** to accept your changes and return to the **DDS-Fieldbus Profile Generator**.
6	Click **Convert** to finalize your changes.
7	The **Success** dialog box opens to confirm your changes: Click **OK** to close the dialog box.

Appendices



Overview

These appendices contain reference material on communications, troubleshooting, and diagnostics.

What Is in This Appendix?

The appendix contains the following chapters:

Chapter	Chapter Name	Page
A	What is BACnet?	147
B	BACnet Troubleshooting and Diagnostics	165
C	Firmware Upgrade Procedures	179
D	SoHVAC Data Types	195

What is BACnet?

A

Overview

This chapter provides an introduction to BACnet.

NOTE: This appendix describes selected BACnet features. BACnet features described herein are not necessarily supported by the TM168BACS or the TM168BACW modules.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
A.1	Introduction to BACnet	148
A.2	BACnet Terminology	149
A.3	BACnet Routers, Gateways, BBMDs, and Foreign Devices	162

A.1 Introduction to BACnet

Introduction to BACnet

About BACnet

The Building Automation and Control Network (BACnet) communication protocol was developed by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers, Inc. (ASHRAE).

BACnet integrates products from different manufacturers in building automation control systems. BACnet allows products from different manufacturers (that meet ANSI/ASHRAE Standard 135-2004) to communicate over a network. These different products include controllers, workstations, actuators, and sensors. In BACnet, each product is known as a device.

BACnet is a common network technology that facilitates communication among many different networked systems. Within BACnet, you can view and configure networks, controllers, classes, objects, and properties in the same way.

NOTE: If you do not already have the ANSI/ASHRAE Standard 135-2004 BACnet, A Data Communication Protocol for Building Automation and Control Networks, you can get it from the website http://www.bacnet.org.

A.2 BACnet Terminology

Introduction

This section provides descriptions of components and terms that are applicable to the use and implementation of BACnet technologies.

What Is in This Section?

This section contains the following topics:

Topic	Page
What is a BACnet Network?	150
BACnet Devices and Device Profiles	151
BACnet Objects	153
BACnet Properties	155
BACnet Services	156
BIBBs	157
BACnet Broadcasts	158
BACnet Command Priority	159
BACnet PICS	161

What is a BACnet Network?

A BACnet network is a transport (LAN or WAN) that carries data from device to device, within a network and between networks. A BACnet network can be a high-speed backbone network:

- Ethernet
- BACnet/IP

It can also be a fieldbus network:

- Master-Slave/Token-Passing (BACnet MS/TP)
- ARCNET
- LonTalk

NOTE: Since many BACnet devices are located across the network on smaller subnetworks, the term *Internetwork* is often used in BACnet literature to describe an entire network of BACnet.

BACnet Devices and Device Profiles

About BACnet Devices

A BACnet device conforms to the BACnet standard. The device can perform these services:

- building controller
- field controller
- router
- gateway
- end device (for example, a sensor or actuator)

Devices in a building are networked as peer-to-peer devices, slave devices, or master/slave devices.

Device Identifiers

This table describes the identifying characteristics of BACnet devices:

Identifier	Description	Valid Numeric Values	
device identifier	This instance number is unique to that device across many different networks that comprise a BACnet system.	1 ... 4194303	
network number	This number is unique to the network to which the device belongs.	1 ... 65535	
MAC address	This address is unique only within its own network.	MS/TP networks:	1 ... 254
		ARCNET networks:	1 ... 255
		Ethernet:	1 ... 281
			474
			976
			710
			655

NOTE: A MAC address is typically read from a DIP switch or from non-volatile memory. Some devices auto-assign MAC addresses when devices are placed on the network.

BACnet devices can have input/output functionality or no input/output functionality.

About Device Profiles

The BACnet standard identifies 6 device types, also known as device profiles:

- BACnet Operator Workstation (B-OWS)
- BACnet Building Controller (B-BC)
- BACnet Advanced Application Controller (B-AAC)
- BACnet Application Specific Controller (B-ASC)
- BACnet Smart Actuator (B-SA)
- BACnet Smart Sensor (B-SS)

BACnet Objects

What Are BACnet Objects?

BACnet objects are the logical representation of system data. Objects represent data that originate in physical inputs, physical outputs, or software processes (for example, single physical points or logical groupings/collections of points) that perform a specific function. Objects standardize the organization of data to facilitate the exchange of data between products from different manufacturers.

Each object possesses a number of properties. The BACnet standard provides these standard objects:

- Accumulator
- Analog_Input
- Analog_Output
- Analog_Value
- Averaging
- Binary_Input
- Binary_Output
- Binary_Value
- Calendar
- Command
- Device
- Event_Enrollment
- File
- Group
- Life_Safety_Point
- Life_Safety_Zone
- Loop
- Multi_State_Input
- Multi_State_Output
- Multi_State_Value
- Notification_Class
- Program
- Pulse Converter
- Schedule
- Trend Log

Individual manufacturers may implement their own proprietary object types, as long as they conform to the BACnet standard.

How Are Objects Identified?

Each object has a numerical object identifier that includes an object type and an instance number:

- Object types 0 to 127 are reserved to identify standard BACnet objects.
- Object types 128 to 1023 are used to identify proprietary objects.
- BACnet devices support object types up to a limit of 4194303 instances. (Instance numbers can be 1 to 4194303.)

BACnet Properties

What Are BACnet Properties?

Objects are examined and controlled by a set of properties that belong to each object. A property contains the smallest piece of BACnet information, and it has a name and a value. For example, a property named high_limit can hold a value of 78.0. A property can be written and/or read, and can provide command control.

For every object, the BACnet standard requires some specific properties while others are optional. Some other properties can be proprietary to a manufacturer. Implement the required properties for each object type. You do not have to implement optional properties, but the optional properties you do implement must conform to the BACnet standard.

Each BACnet Device object contains properties that can be used to verify communications, identify the vendor, identify the software and firmware revision, and other characteristics of the device. The device properties of the device object represent the externally visible characteristics of a BACnet device.

How Are Properties Identified?

Each property has a numeric property identifier. Properties 0 to 511 are reserved as standard, though only 166 properties are currently defined in the BACnet standard. Properties 512 and higher are unique proprietary properties set by the manufacturer.

Vendor ID is the device object property that identifies the manufacturer.

BACnet Services

Introduction

BACnet services are essentially the messages that BACnet devices send to each other. These services are provided:

- Read and write the property values of one or more objects.
- Send notifications of BACnet Alarm signals and BACnet Events.
- Read and write files.

Services follow a basic client/server model. A BACnet client is a device that requests a service. A BACnet server is a device that performs a service. Refer to the discussion of BACnet Broadcasts *(see page 158)*.

Services

These are the major BACnet service categories:

Category	Service
Alarm and Event	BACnet alarm routing and event notification
File Access	Access and manipulate files within devices.
Object Access	Read and write properties.
	Create and delete objects.
	Manipulate lists of data.
Remote Device Management	Remotely monitor and control devices.
Virtual Terminal	Establish (for a client user) a connection to an application program server in another BACnet device.

BIBBs

What are BIBBs?

BACnet Interoperability Building Blocks (BIBBs) are collections of BACnet services. They represent the next detailed layer of service components.

BIBB Categories

BIBBs are grouped into these major categories:

- data sharing
- BACnet Alarm and BACnet Event management
- device and network management

Different combinations of BIBBs apply to each type (profile) of BACnet device (B-OWS, B-BC, B-AAC, B-ASC, B-SA, B-SS). The BIBB services provided for a B-ASC type of device are summarized in this table:

Category	Capabilities and Services Provided for a B-ASC
Data Sharing	Provide the value of any of its BACnet objects.
	Modify some BACnet objects in other devices.
BACnet Alarm and Event management	Enables the user to determine in advance how to handle BACnet alarms and BACnet events as they occur during runtime
Device and Network Management	Respond to queries about its status
	Respond to requests for information about any of its objects.
	Respond to communication control messages.

BACnet Broadcasts

BACnet Broadcast Types

A BACnet broadcast is a broadcast that carries messages (or services) from one device to another. BACnet broadcasts include these types:

- `Who-Is`: A device uses this query to discover other BACnet devices and their objects.
- `I-Am`: A device uses this type to identify itself and its objects to other devices.
- BACnet alarm messages are delivered to devices.
- Messages inform devices that the value of one or more devices has changed.

Sending and Receiving BACnet Broadcasts

On an IP network, broadcasts are sent and received through a UDP port on each device. The default port number is [0xBAC0]. They are also sent using an IP router and a BACnet Broadcast Management Device (BBMD).

BACnet Command Priority

Introduction

In your building control system, an object can be manipulated by a number of different entities. The current value of an object is set by several applications and other sources.

Each application has a well-defined function to perform. When the actions of 2 or more applications conflict with regard to the value of an object property, there is a need to arbitrate between them.

Arbitration allows several program and non-program sources to manipulate the value of the same object. For example, a start/stop program can command a particular `BinaryOutput` to turn on while a demand-metering program can command the same `BinaryOutput` to turn off. In this case, the OFF command takes precedence. However, an operator can override the demand-metering program and force the `BinaryOutput` to on.

Command Priority Process

Arbitration in BACnet is provided by a process known as Command Priority, which assigns varying levels of priorities to commanding entities throughout the system. Each object that contains a commandable property is responsible for acting on prioritized commands in the order of their established priorities.

Implementation of the command priority process involves these command priority properties:

- **Commandable Property**: Each object that supports command priorities has one or more commandable properties. The values of these properties are controlled by the command priority process.
- **Priority_Array:** BACnet has established a set of 16 priority levels called the priority array. The array consists of commands or NULLs in an order of decreasing priority. The highest priority (lowest array priority level) with a non-NULL value is the active command. If a priority level holds a value of NULL, the next non-NULL is assigned to the object.
- **Relinquish_Default:** When all priority levels in the priority array become NULL, the value of **Relinquish Default** is assigned to the commandable property. You set the value of **Relinquish Default** when you configure the BACnet object.

Command Values and NULLs

A priority level in the priority array can have a commanded value or a NULL value. A NULL value indicates that there is no existing command at that priority. An object continuously monitors (polls) the entire priority array to locate the entry with the highest non-NULL value. It then sets the commandable property to this value.

Relinquishing a Command

A commanding entity (for example, an application program or operator) can send a command to a commandable property of an object. It can also relinquish an older command with a writer operation. That write operation is similar to the command itself, except that the value of NULL is commanded. That is, relinquishing a command places a NULL value in the priority array corresponding to the appropriate priority. (You can override and relinquish a commanded value.)

BACnet Command Priority Array

This is the 16-level BACnet priority array. The first 2 priorities are related to personnel safety. (Refer to the BACnet standard for complete descriptions of these priorities.)

1	Manual-Life Safety
2	Automatic-Life Safety
3	priority 3, available
4	priority 4, available
5	Critical Equipment Control
6	Minimum On/Off
7	priority 7, available
8	Manual Operator
9	priority 9, available
10	priority 10, available
11	priority 11, available
12	priority 12, available
13	priority 13, available
14	priority 14, available
15	priority 15, available
16	priority 16, available

NOTE: If an attempt is made to command a property for which a priority level is not specified, a default priority level of 16 (the lowest priority) is assumed. If an attempt is made to command a property that is not commandable with a specified priority level, the priority is ignored.

BACnet PICS

Introduction

BACnet Protocol Implementation Conformance Statements (PICS) are detailed descriptions of the inherent BACnet capabilities of a device. PICS are available from each BACnet manufacturer.

Functions of PICS

PICS can perform these functions:

- Identify to a potential user those objects and BACnet services that a device supports.
- Detail the communications network type, the baud rate, and the range of values each object property expects.
- Specify whether a property is writable or read-only.
- Assess the level of interoperability among devices.

A.3 BACnet Routers, Gateways, BBMDs, and Foreign Devices

Introduction

This section describes BACnet devices such as routers, gateways, BBMDs, and foreign devices.

What Is in This Section?

This section contains the following topics:

Topic	Page
BACnet Routers and Gateways	163
BBMDs and Foreign Devices	164

BACnet Routers and Gateways

Introduction

This is a discussion of routers and gateways on BACnet networks.

NOTE: Exchanges of BACnet information through routers and gateways are sometimes referred to as internetworking.

Routers

A router (or IP router) is a BACnet device (such as Andover Continuum bCX1 from Schneider Electric) that facilitates the exchange of data between different types of BACnet networks (MS/TP, BACnet/IP, Ethernet, etc.). A router is simply a pass through device that does not change the data format or the content of the message. The use of a router to exchange broadcast messages between networks requires the implementation of 1 BACnet Broadcast Management Device (BBMD) per network.

For more information on BBMDs, refer to BBMDs and Foreign Devices *(see page 164)*.

Gateways

A BACnet gateway device facilitates the exchange of data between devices on a BACnet network and devices on a non-BACnet network to share BACnet and non-BACnet information. While a router simply passes information from one network to another, a gateway takes the data from one device, analyzes it, translates the data into another data protocol (BACnet or non-BACnet), and delivers it. The destination device, therefore, understands the message.

Physically, a gateway can take one of these forms:

- *internal*: This is typically a board or module inside a device.
- *external hardware/software*: This is typically an external hardware interface box combined with a software translator.
- *software*: This is typically a software translator on a PC.

BBMDs and Foreign Devices

BBMDs

A BBMD is a workstation (B-OWS) specially designated to deliver broadcast messages through one or more routers between BACnet networks. (Refer to the discussions of routers and gateways *(see page 163)* and BACnet broadcasts *(see page 158)*.)

Each network must have a BBMD. Each BBMD maintains 2 internal tables:

- **Broadcast Distribution Table (BDT):** A BDT maintains a list of other BBMDs located on other foreign networks. When a foreign BBMD is added to a BDT, it becomes registered in the local BBMD. During this process, not only does the foreign BBMD get registered, but all BBMDs listed in its foreign BDT also get registered. This means that the local network knows about the foreign network and all the networks that the foreign network knows about.
- **Foreign Device Table (FDT):** An FDT maintains a list of foreign devices. A foreign device is simply the identity of a device residing on another BACnet network. When a foreign device is added to an FDT, it becomes registered with the local BBMD.

The BDT and FDT tables allow different networks to recognize each other and their respective devices. Such recognition must be achieved before broadcast messages are routed.

Broadcast Messages

In your BACnet system, you can designate and register BBMDs (and foreign devices). That allows broadcast messages to be routed among BACnet networks.

Foreign Devices

Foreign Device: A foreign device is a BACnet device with an IP subnet address that is different from the subnet address of the BACnet/IP network the device seeks to join.

BBMD Operation: For a foreign device to participate fully in the activities of a BACnet/IP network, the device must register itself with a BBMD serving one of the IP subnets comprising that network. "Full participation" implies the ability to send and receive directed and broadcast messages. Ascertaining the IP address of such a BBMD is a local matter but could involve the use of a domain nameserver or the distribution of a numeric IP address to authorized users. The UDP port X'BAC0' is the default, but the use of other port values is permitted when they are required by the local network architecture (such as when 2 BACnet/IP networks share the same physical LAN).

BACnet Troubleshooting and Diagnostics

B

Overview

This chapter describes common scenarios you may encounter in a BACnet environment.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
B.1	General Troubleshooting	166
B.2	Diagnostics	167

B.1 General Troubleshooting

Troubleshooting Tasks

CPU Indicator Not Flashing

The network status (**NS**) indicator does not flash when the unit is not operating. This could be because primary power has been lost or there has been another detected internal dysfunction.

Confirm that you have configured the application for the correct protocol (BACnet MS/TP or BACnet/IP) using the SoHVAC software. A BACnet IP module does not operate when it is configured for BACnet MS/TP communications (and vice-versa).

Make sure that power is available and connected properly to the power terminals on the controller. This can be done using a multimeter reading the voltage across the positive and negative terminals.

Functioning Unit Does Not Respond

The unit is usually operational when the network status (**NS**) indicator flashes normally. However, keep in mind that it will not respond if it detects an invalid configuration parameter. The module starts only if the configuration settings are valid.

Before you compile your application in SoHVAC, confirm that you have generated the BACnet profile *(see page 140)* with the **Tools** → **BMS Configuration** → **Generate BACnet profile** command.

RS-485 activity: RS-485 communications can be monitored by observing the status of the TXD (transmit) and RXD (receive) LED indicators. During communications, both LEDs should show activity.

Ethernet activity: A flashing Link/Activity LED indicates ongoing Ethernet communications. You can use a sniffer program (such as Wireshark, www.wireshark.org) to monitor Ethernet traffic to and from the module.

Inoperable Input or Output

If the network status (**NS**) indicator and other inputs and outputs are operating properly, check the status of these items:

- The input or output is detected as damaged. In this case, contact a Schneider Electric representative for assistance.
- The program that controls the inputs and outputs may not be correct (especially if this is the first time you are using the controller). Check your program.

B.2 Diagnostics

Introduction

The topics in this chapter help you diagnose some of the situations that can occur when implementing a controller.

What Is in This Section?

This section contains the following topics:

Topic	Page
No Communications with a New BACnet MS/TP Device	168
No Communications with a New BACnet/IP Device	170
Slow or Intermittent Communications with a BACnet MS/TP Segment	171
Communication Timeout	172
Slow Segments	173
BACnet Cannot Discover All Devices	174
Workstation Does Not Receive BACnet Alarm Signals	175
Undiscovered BACnet Device Objects	176
Unreadable Object Properties	177
Multiple BACnet Client Tools on PC	178

No Communications with a New BACnet MS/TP Device

Symptom

A new BACnet MS/TP master or slave device on the network cannot be reached or discovered or it does not respond to the tools trying to find it.

Solutions for Master Devices

Use a BACnet tool to generate a `Who-Is` request. The device should respond with an `I-Am` response, indicating that it is reachable and discoverable.

Perform one of these tasks when the master device does not respond to `Who-Is`:

- Check the PICS to verify device support for `DM-DDB-B`.
- Use a BACnet MS/TP sniffer to check that the MAC address of the device is receiving token pass (TP) messages. If not, check that other BACnet MS/TP master devices are sending PollForMaster (PFM) messages to that MAC address. Typically this is the device whose MAC address is one lower than the device that is not responding. For example, perform this sequence of checks when MAC 05 does not respond:
  - Make sure that MAC 04 is sending PFM to MAC 05.
  - Make sure that MAC 05 is replying with RPFM.
  - Make sure MAC 04 sends TP to MAC 05.

NOTE: If MAC 04 does not send a PFM or a TP, its MaxMaster setting may be lower than the non-responding device (MAC 05). In this case, make the MaxMaster for each device on the BACnet MS/TP segment at least as large as the MAC address of the non-responding device.

If the above settings are OK and the device still does not respond, check these possibilities:

- The sending device (MAC 04 in this example) is dropping TxEnable too quickly, which produces a CRC mismatch in the message. In this unlikely event, the event should be visible in the sniffer trace.
- The sending does not honor the Tturnaround (40 bit times minimum silence) when it receives the token. In this case, the PFM or TP is sent too early. (This unlikely event is measured only with a digital oscilloscope.)
- The EIA-485 polarity is reversed.
- The BACnet MS/TP speed setting is mismatched.
- The MAC address is not set correctly.
- The inoperability of a device is detected (an open wire, shorted wire, nonoperational device, etc.). Wires that are open or shorted can affect other devices on the BACnet MS/TP segment. In this case, you can rule out an overall system inoperability by successfully communicating with other devices.

Solutions for Slave Devices

Slave devices cannot be discovered using dynamic device binding unless there is a BACnet MS/TP proxy device. Proxies have to be enabled to do proxying according to proprietary procedures for that device.

For slave devices that are reached by static binding but do not respond to requests (such as `ReadProperty`), use a BACnet MS/TP sniffer to determine if there is any response at all.

There may be no response under these conditions:

- The sending device is dropping TxEnable too quickly, which causes CRC mismatches in the message. This unlikely event should be visible in the sniffer trace.
- The sending is not honoring Tturnaround (40 bit times minimum silence) when it gets the token. In this case, it sends the PFM or TP too early. (This unlikely event is measured only with a digital oscilloscope.)
- The EIA-485 polarity is reversed.
- The BACnet MS/TP speed setting is mismatched.
- The MAC address is not set correctly.
- The inoperability of a device is detected (an open wire, shorted wire, nonoperational device, etc.). Wires that are open or shorted can affect other devices on the BACnet MS/TP segment. In this case, you can rule out an overall system inoperability by successfully communicating with other devices.

There may be a response under these conditions:

- The header or data CRC mismatch could be caused by dropping TxEnable or detected Tturnaround issues. Duplicate MAC addresses can exhibit similar symptoms because the replies from 2 devices can be slightly unsynchronized.
- The response may be taking too long. A response slower than 255 ms causes the sender to give up waiting for a `DataExpectingReply` frame.

No Communications with a New BACnet/IP Device

Symptom

A new BACnet/IP device on the network cannot be reached or discovered or it does not respond to the tools trying to find it.

Possible Solutions

Determine whether the BACnet/IP device is operating at the expected IP address:

1. Send a ping command to the expected IP address.
2. Confirm the device response.

If no ping response is received, verify the IP address of the device by using a sniffer to capture and read the Ethernet traffic the device transmits when it boots up. This traffic should include a gratuitous ARP transmission that contains the IP address of the device.

Use a BACnet tool to generate a `Who-Is` request. The device should respond with an `I-Am` response, indicating it is reachable and discoverable.

Confirm that the BACnet/IP device has at least one Link/Activity LED that is on or flashing.

Slow or Intermittent Communications with a BACnet MS/TP Segment

Symptom

The response from a specific BACnet MS/TP segment is very slow, for example, when compared to a similar BACnet MS/TP segment on another floor of the same building. Alternately, the communication to devices on the segment may be intermittent.

Solutions

Diagnosis	Action
The **MaxMaster** value exceeds that of the device with the highest MAC address. That is, a sample MAC address is 00, 01, 02 … 29 while the MaxMaster is greater than 29. Therefore, end node(s) spend time hunting for missing master devices every 50 token cycles.	In the example case, set the MaxMaster to 29 (the highest implemented MAC address). If some nodes cannot change their MaxMaster (the default is 127), arrange the application so that the highest MAC address is used by a device where the MaxMaster can be changed.
There are gaps in MAC address assignments.	Close the gaps.
The node with the highest MAC address (the end node) has a lenient or strict Tusage_timeout policy. When there are unused master MAC addresses combined with an end node that is lenient in its policy, every millisecond of leniency time is multiplied by the number of unused master MAC addresses every 50 cycles. This results in periods of no activity on the network, the visible effect of which is slow overall response on that segment.	Adjust the Tusage_timeout policy to avoid this situation.
CRC mismatches occur during communications with particular nodes. This becomes evident when you examine the network statistics in client devices or use a BACnet MS/TP sniffer.	A higher frequency of detected errors suggests the presence of other detected issues: • If baud rates are mismathced for TxEnable or Tturnaround, modify the settings. • If there is improper or marginal network biasing, check the termination and biasing of the network. A lower frequency of detected errors (only a few per day) suggests a disturbance (noise), in which case you need to check the wiring.
Framing errors result from collisions, especially while specific nodes are communicating. Use a BACnet MS/TP sniffer to see this. Framing errors can indicate mismatched baud rates, marginal network biasing, etc. They can also cause dropped tokens, which are indicated by 500 ms+ gaps.	Check the network biasing and, if necessary, modify Tturnaround and/or TxEnable timing.

Communication Timeout

Symptom

The following actions are suggested when communications are intermittent or they frequently time out.

Solution for a Timeout with a Specific Device

Diagnosis	Action
Communication to a specific device is intermittent or times out (no response within a few seconds).	Retry the communication: ● Refer to the topic No Communications with a New BACnet MS/TP Device *(see page 168)*. ● Check to see if the burst rate is exceeded for the device.

Solutions for a Timeout with All Devices

Diagnosis	Action
The router is overloaded with traffic.	Use a sniffer to monitor the client side of the router to see if it generates `Router-Busy-to-Network` messages. If it does, a high volume of traffic could create too many `Who-Is` requests or other broadcast traffic. If no such messages are generated for a BACnet MS/TP segment, perhaps the MaxInfoFrames for the BACnet MS/TP port on the router is too low. (Usually it should be 50 or higher.)
There is a detected issue downstream of the router on a segment other than the client side segment to the router.	Check the timing settings of the nodes connected in that segment.

Slow Segments

Symptom

A segment with 2 or more routers connected to it is very slow. A sniffer shows continuous `Who-Is` and `I-Am` broadcast traffic.

Solutions

Diagnosis	Action
circular routes	Check for circular routes. Often, 2 routers are mistakenly connected to the same Ethernet segment, both of which have Ethernet 8802-3 and BACnet/IP ports. Only one of the routers can have routing to both ports enabled. (The other router must disable routing to one of the ports.) Otherwise a circular route is created, even if the network numbers are different. Look at the HopCount in sniffer traces of routed `Who-Is` messages. The HopCount starts at 255 and is decremented each time the message is routed to another segment. Typical networks only have 2 or 3 levels, so HopCounts of less than 252 indicate that the message is circulating more than once through routers.
broadcast storms	Check for broadcast storms. It is possible to send `Who-Is` messages without a qualifying range of device instance numbers, but the broadcast of unqualified `Who-Is` messages globally can create a large amount of responding `I-Am` traffic. Such traffic can overwhelm routers and BACnet MS/TP networks. Use the sniffer to look for a `Who-Is` message that does not have a range qualification to find the sending device.

BACnet Cannot Discover All Devices

Symptom

BACnet discovery is based on broadcast messages. IP limits the delivery of broadcasts to nodes in the same IP subnet. Your BACnet network can discover some BACnet/IP devices, but not others.

Solution

Diagnosis	Action
All BACnet/IP devices are not on the same IP subnet.	Place an IP router between the subnets. One of these conditions must be true: ● There is a BACnet broadcast management device (BBMD) on each subnet, and each BBMD is configured to know the IP addresses of every other BBMD. ● All of BACnet/IP devices on subnets other than the one with the BBMD have registered with the BBMD as foreign devices. ● Each BACnet/IP client uses static binding instead of discovery.

Workstation Does Not Receive BACnet Alarm Signals

Symptom

An operator workstation is not receiving BACnet Alarm signals.

Solution

The Notification Class object in the detecting device must meet these conditions:

- It knows the network and MAC address of the workstation through static binding or the device instance and use dynamic binding.
- It has a processID that is recognized by the workstation.
- It has a notification class that is recognized by the workstation.
- It has ValidDays and FromTime/ToTime that match the period when the notification signal is sent.
- It has a destination transition that matches the transition that has occurred (for example TO-OFFNORMAL).

The source object that generated the transition must have a matching Event_Enable for that transition (and a matching Limit_Enable in the case of analog Out_Of_Range).

With a sniffer, verify that the device is generating the EventNotification. Confirm that the notification is also arriving at the workstation by sniffing at the workstation and source device. This of particular importance if there are one or more intervening routers.

Undiscovered BACnet Device Objects

Symptom

A workstation or BACnet tool is able to discover a particular BACnet device, but not the objects in it.

Diagnosis

BACnet clients typically discover devices using Who-Is and dynamic device binding. This procedure locates the network and MAC address of the device and its device instance. To discover objects in the device, the client typically uses ReadProperty or ReadPropertyMutliple to read the Object_List property of the device object. Several common unintended events can occur in this procedure, mostly arising from the client or server implementation. The client tries to use ReadPropertyMultiple, but the device does not support this and reports an event. The client then gives up. One of the following is also true:

- The client tries (falls back to) ReadProperty to read the entire Object_List property. The Object_List is larger than 92 objects and the server returns a segmented response, but the client cannot support segmentation so it gives up.
- The Object_List is larger than 92 objects and the server does not support segmentation. In this case, it returns notice that it has detected an event (segmentation not supported) and the client gives up.
- The client sees that segmentation is not supported (or immediately uses this procedure and does not try to read Object_List without an array index). It instead reads Object_List[0] to get the number of objects, then Object_List[1 to N], reading the object list one by one. However, one of these situations must also be true:
  - The server improperly handles Object_List[0] and reports a detected event or times out. The client gives up.
  - The server improperly handles Object_List[x] and reports a detected event or times out. The client gives up.
  - The server takes too long to reply to Object_List[x], which appears to be a timeout. The client gives up.

All of these detected events are without field solutions because they are caused by an incorrect BACnet implementation in the client or server. Use the sniffer to capture the traffic, evaluate the situation, and get the appropriate vendor to fix the BACnet product.

Unreadable Object Properties

Symptoms and Solutions

A BACnet client is able to read some object properties, but not a particular object or property from a device:

- Verify that the device contains the object you are trying to read. Check the PICS.
- Verify that the object of that object type supports the property you are trying to read. Check the PICS.
- Use a sniffer to verify that the device is returning the specified property. If not, that indicates a detected problem with the device implementation. If it returns the property value, the BACnet client may not support that property datatype. This is more common for complex datatypes such as the Schedule object and Exception_Schedule property.

Multiple BACnet Client Tools on PC

Symptoms

There are detected problems using multiple BACnet/IP client tools on the same Windows PC.

Most Windows-based BACnet clients use the Winsock interface. When such programs are running, they attach themselves to the standard BACnet UDP port 0xBAC0 (47808) and listen for incoming BACnet messages on that port. Unfortunately, only one program can listen on this port at a time. So when a program is active (for example, a running Windows Service), other BACnet tools cannot share the use of the UDP port.

Solutions

- Turn off the other tool or service.
- Use a second Ethernet interface with a different IP address on the same subnet so that each program has its own IP address and UDP port combination.
- Remember that a small number of BACnet applications attach themselves to all available IP adapters and UDP port BAC0. If you use this kind of program, monitor the number of ports being used by each application to avoid port contention.

Firmware Upgrade Procedures

C

Getting Started

This appendix describes how to upgrade the firmware of your TM168BACS, TM168BACW, or TM168MODW module.

What Is in This Chapter?

This chapter contains the following sections:

Section	Topic	Page
C.1	Upgrading the TM168BACS	180
C.2	Upgrading the TM168BACW and TM168MODW Modules	184
C.3	Upgrading the TM168MODW Firmware	192

C.1 Upgrading the TM168BACS

Downloading Firmware to a TM168BACS With BACbeat

Introduction

Upgrade the firmware for the TM168BACS module over BACnet using a tool with these functions:

- Write to the file object.
- Execute the BACnet `ReinitializeDevice` command.

The following example uses the BACbeat software tool from PolarSoft (http://www.polarsoft.biz/index.html).

NOTE: The TM168BACS module reboots during the firmware upgrade process. You will lose BACnet communications for up to 1 minute during the upgrade.

Connecting a PC to the TM168BACS

When you use PolarSoft's BACbeat software, connect your PC to the TM168BACS module. Make the connection with one of these methods:

- Connect the BACnet MS/TP port on the module using the serial port on your PC and an RS232/RS485 converter.
- Connect to the Ethernet port on your PC and a BACnet/IP-to-BACnet MS/TP router.

Make sure the TM168BACS module is plugged into the Modicon M168 controller when power is applied. You can monitor communications over BACnet MS/TP with BACbeat.

Required Files

To enable the module to upgrade its firmware, load these files to the file system over BACbeat:

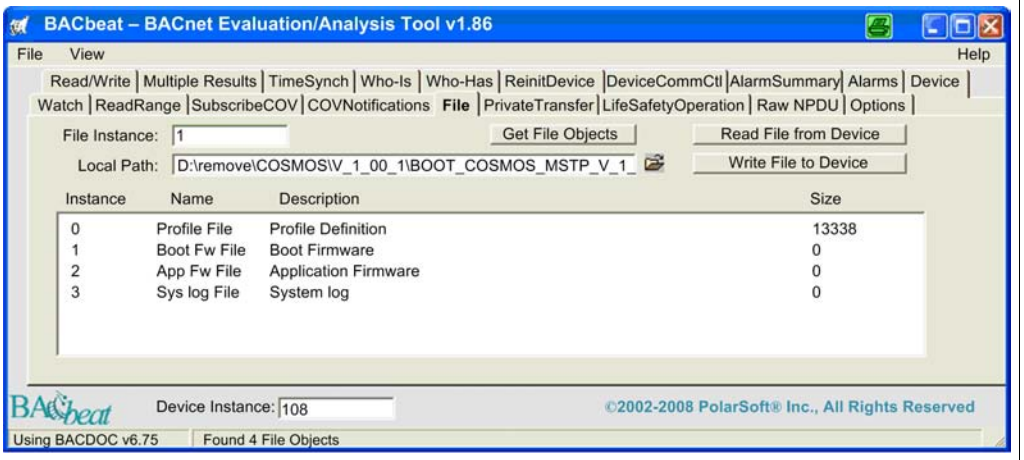
- boot code
- application code

These are the file names in this example:

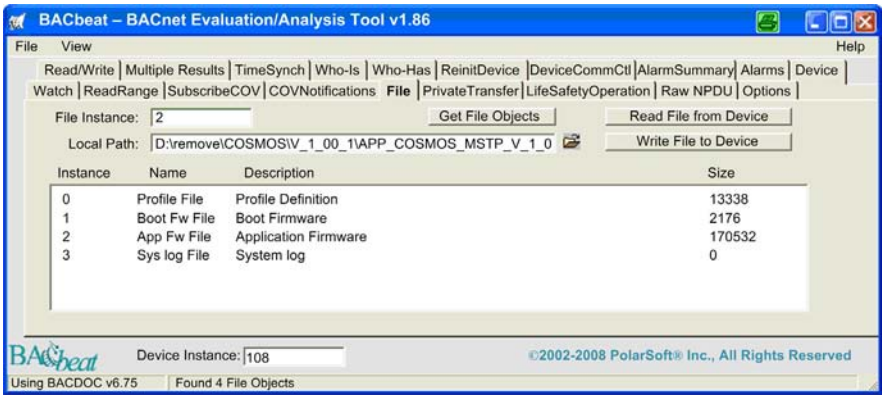
- boot: `BOOT_COSMOS_MSTP_V_1_01_1.hms`
- application: `APP_COSMOS_MSTP_V_1_00_1.hms`

Performing the Transfer

Transfer the application code and boot code to the module:

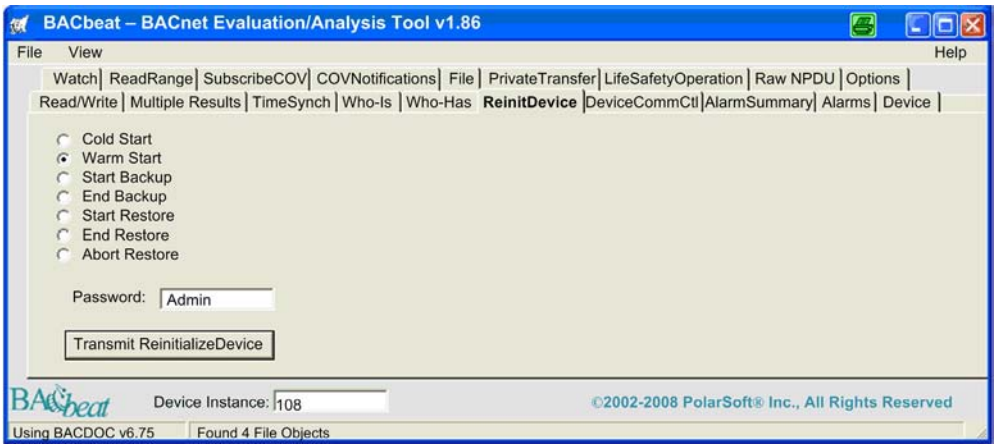
Step	Action
1	Open the **File** tab in the BACbeat screen, and select **Get File Objects** to read and display the current content of the file system in the module. 
2	Transfer the boot code to the module: • In the **Local Path** field, navigate to the location for the boot file on your PC. • Type the number 1 in the **File Instance** field. • Click **Write File to Device**. **NOTE:** It may take several minutes to complete the download at 38400 baud, and longer at slower speeds. Instance 1 in the list is updated.
3	Transfer the application code to the device: • In the **Local Path** field, navigate to the location for the APP file on your PC. • Type the number 2 in the **File Instance** field. • Click **Write File to Device**. **NOTE:** It may take several minutes to complete the download at 38400 baud, and longer at slower speeds. Instance 2 in the list is updated.

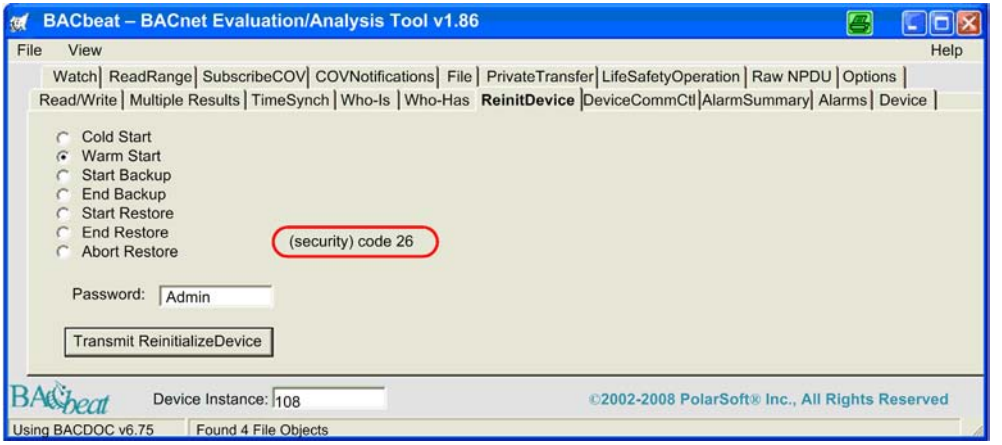
After the transfer of both files, the screen looks like this:



Re-Initializing the Device

Reinitialize the module to complete the firmware installation:

Step	Action
1	In the BACbeat software, open the **ReinitDevice** tab: 
2	Perform these steps on the **ReinitDevice** tab: **a.** Select **Warm Start**. **b.** Type in the **Password** (in this case `Admin`). **c.** Click **Transmit ReinitializeDevice**. The module requests a reboot from the controller. When this request is granted, the module reboots to complete the firmware installation. During installation, the **MS** LED on the module flashes green and red.

Step	Action
3	Confirm a successful firmware upload using the BACbeat software with one of these methods: ● Open and refresh the **File** page and click **Get File Objects**. The instance 1 and instance 2 file size should be 0. ● Open the **Device** page and click the **Read All** tab to check the firmware version.
4	To detect an unsuccessful firmware upload, look for the response **(security) code 26**. If this response is displayed, the firmware upgrade did not occur: 

C.2 Upgrading the TM168BACW and TM168MODW Modules

Getting Started

This section describes how to update the firmware for the TM168BACW or TM168MODW connectivity module with Unity Loader.

NOTE: These modules reboot during the firmware upgrade process. You may lose communications for up to 1 minute during the upgrade process.

What Is in This Section?

This section contains the following topics:

Topic	Page
Downloading and Installing Unity Loader	185
Update the TM168BACW or TM168MODW Firmware with Unity Loader	186

Downloading and Installing Unity Loader

Introduction

The Unity Loader software utility for Windows must be installed on your PC before you can update the firmware for the TM168BACW or TM168MODW connectivity module.

Procedure

Download the Unity Loader software to your PC:

Step	Action
1	Enter the web address for Schneider Electric (www.schneider-electric.com) in an Internet browser.
2	In the **Search form input field**, enter the phrase **Unity Loader** and press `Enter`.
3	Navigate through the list of search results and select the appropriate entry for the Unity Loader software. **NOTE:** It may be helpful to select the **Download** → **Softwares** menu command to filter the results.
4	Follow the on-screen instructions to download the Unity Loader installation software and any necessary installation instructions to your PC.
5	Run the Unity Loader setup file and follow the on-screen and downloaded instructions to install Unity Loader.

Update the TM168BACW or TM168MODW Firmware with Unity Loader

Before You Begin

Take these preliminary steps before using the Unity Loader software to update the TM168BACW or TM168MODW connectivity module firmware:

- Disconnect the controller from the network.
- Configure the IP addresses of both the module and your configuration PC so that they share the same IP subnet address.

NOTE:

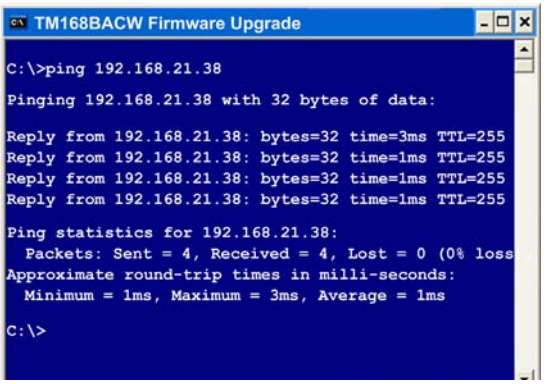
The firmware download process should not be interrupted once it has begun:

- Do not power off your PC when firmware is downloading.
- Do not shut down the Unity Loader software when firmware is downloading.

If the firmware download process is interrupted, the new firmware is not installed and the controller continues to use the old firmware.

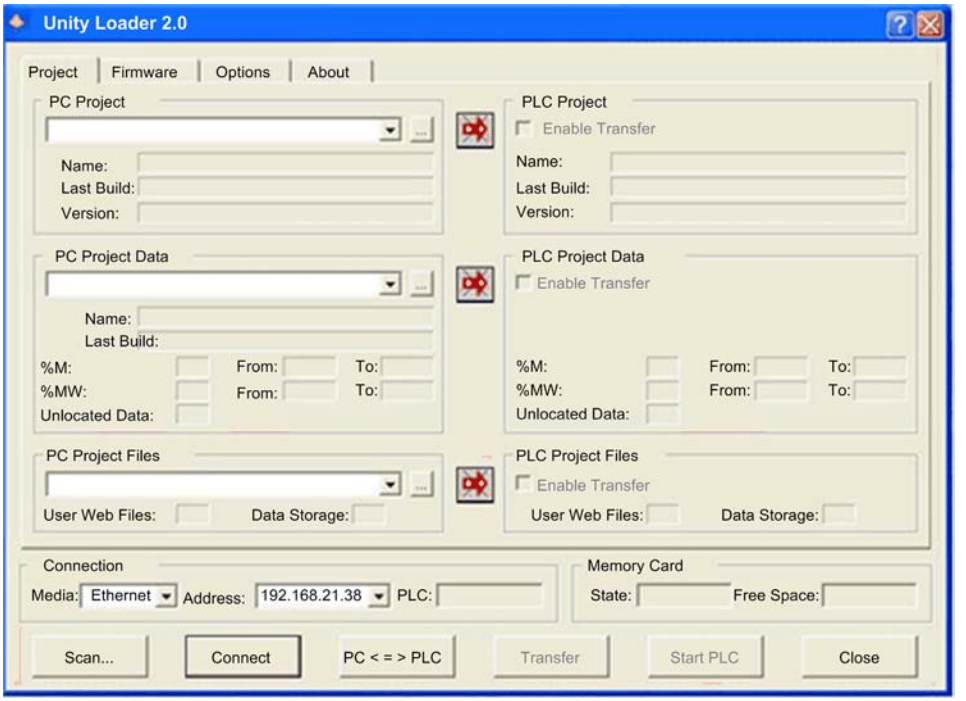
Connecting to the Module

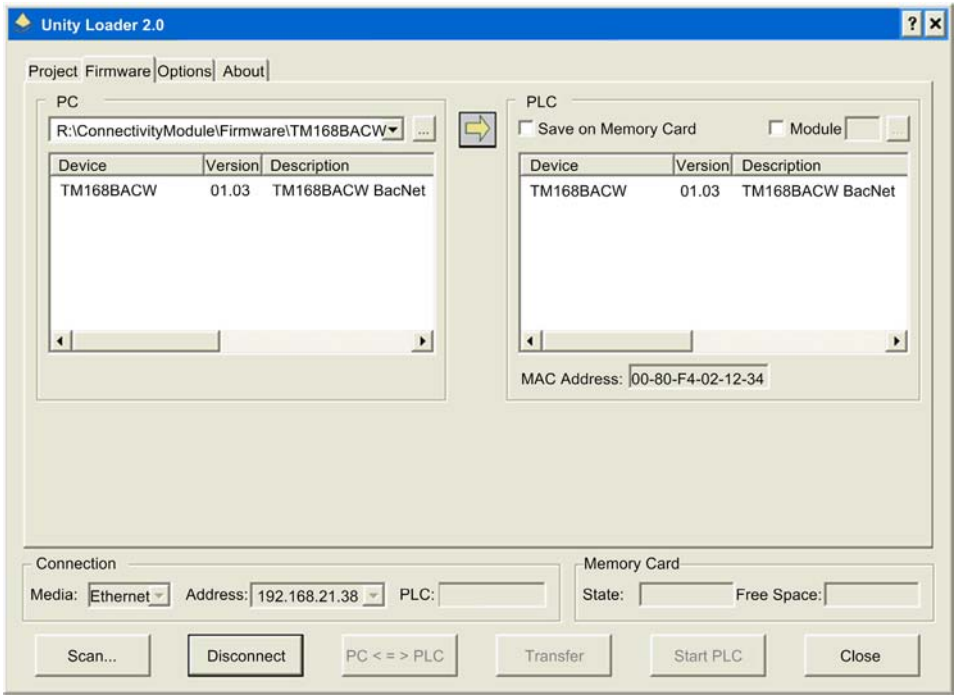
Connect your configuration PC to the TM168BACW or TM168MODW module:

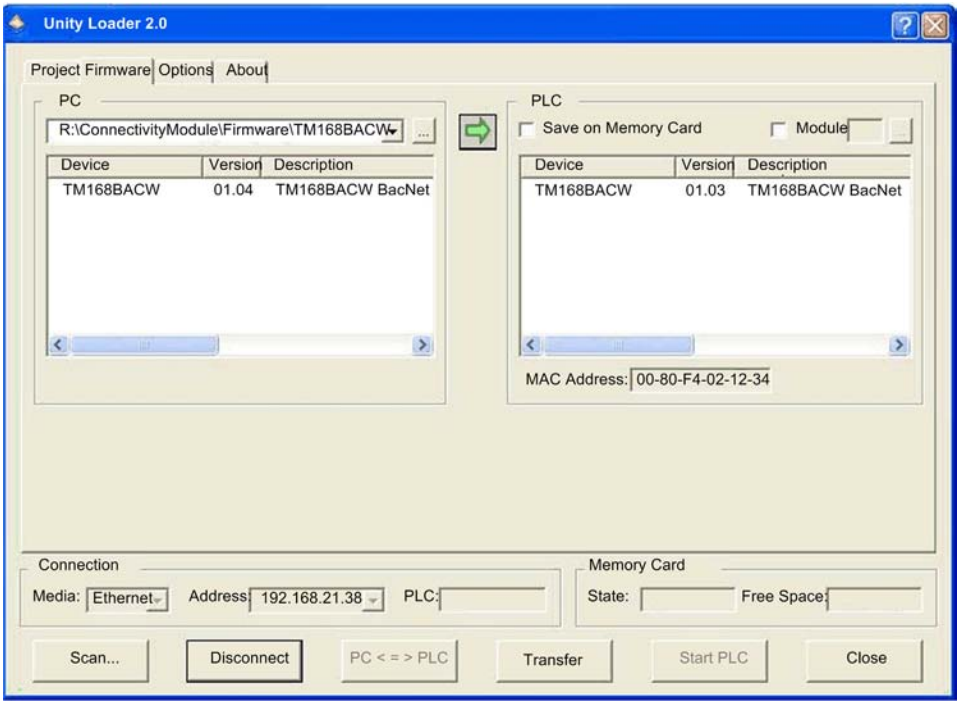
Step	Action
1	You can connect the configuration PC to the device directly or indirectly: ● *direct*: Connect the PC to one of the 2 Ethernet ports on the connectivity module. ● *indirect*: Connect the PC through your Ethernet network infrastructure.
2	Verify that communications are established between the PC and the module with a Ping command from the PC to the module: **a.** Open a command window on the PC (**Start** → **Run**). **b.** In the **Run** dialog, type **cmd** and click **OK**. **c.** At the command prompt, type a ping command and the device IP address. For example: `C:\>ping 192.168.21.38`. The response looks like this for an established connection: 

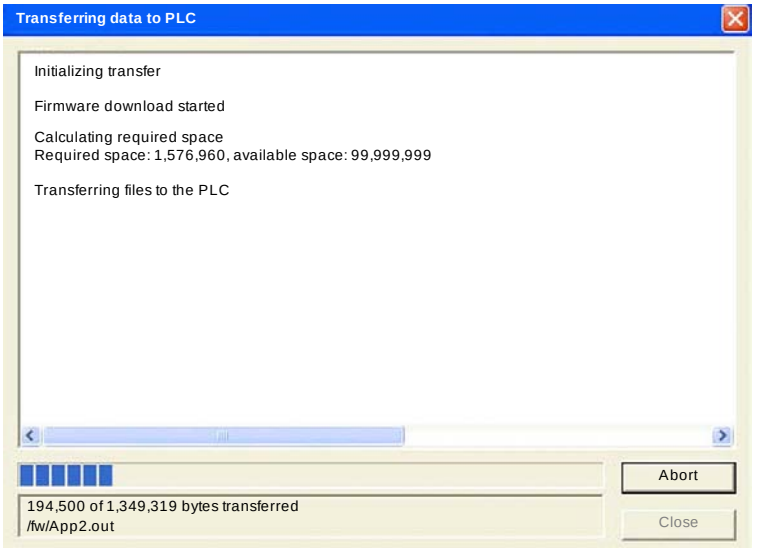
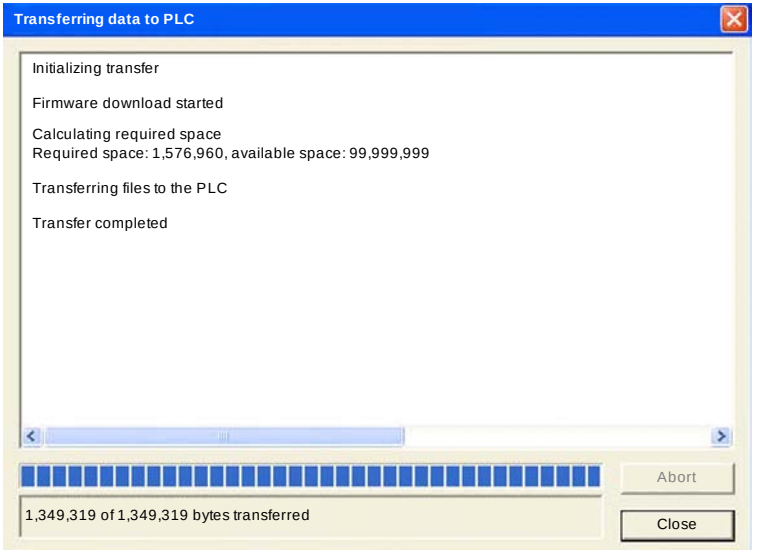
Transferring Firmware to the Connectivity Module

Open Unity Loader on your PC and update the firmware for the TM168BACW or TM168MODW connectivity module:

Step	Action
1	Open Unity Loader on your PC (**Start** → **Programs** → **Schneider Electric** → **Unity Loader**). Unity Loader opens and displays the **Project** tab: 
2	Connect to the module: **a.** Go to the **Connection** area of the **Project** page. **b.** In the **Media** list, select **Ethernet**. **c.** In the **Address** field, type in the connectivity IP address of the module. **d.** Click the **Connect** button.

Step	Action
3	After Unity Loader connects to the module, click the **Firmware** tab: 

Step	Action
4	In the **PC** area of the **Firmware** tab, click the ellipsis (**...**) button to open a dialog where you can navigate to and select the firmware file for the network connectivity module. The firmware is contained in a Unity Loader file with the .LDX file extension. After you select the firmware file and close the dialog, the selected revision of this firmware is displayed in the list on the left and the current version of the firmware is displayed in the list on the right: 
5	Make sure the arrow in the middle of the screen is green and click **Transfer**. **NOTE:** Only click **Transfer** when the arrow is green. A yellow arrow indicates that the firmware on your computer is the same or newer version than the file selected for transfer. A red arrow indicates that the firmware on the computer is not compatible with the Modicon M168 controller. **NOTE:** Do not use the **Stop PLC**/**Start PLC** button when updating firmware for the network connectivity module.

Step	Action
6	Click **yes** on the 2 pop-up windows that appear. A third window indicates the transfer status with the blue bars at the bottom of the screen. 
7	When the transfer is complete, click **Close**. 

Step	Action
8	In the Unity Loader software, click **Disconnect** and close the window. (The connectivity module is shown in the screen above as an example.)
9	Reboot the module to finalize the firmware update. (The configuration and IP settings of the module do not change after the reboot.)

C.3 Upgrading the TM168MODW Firmware

Update Firmware with Windows Explorer FTP

Introduction

Schneider Electric occasionally revises and improves firmware for its products. When new firmware is available, you can install it on your module or device through this process:

Stage	Description
1	Download the new firmware.
2	Locate the firmware files currently running on your device or module.
3	Overwrite the current firmware with the newly downloaded firmware.
4	Cycle power to the module or device.

These stages are described in detail below.

Download the New Firmware

Get the new firmware for your module or device from Schneider Electric:

Step	Action
1	Open Internet Explorer. (The firmware upgrade may not work with other Internet browsers.)
2	Go to Schneider Electric's PI@net home page (planet.schneider-electric.com).
3	Enter the name of your product range.
4	Press the **Software/Firmware** link.
5	Follow the directions to download the new firmware to your local drive.
6	Make a record of the location of the new firmware on your local drive.

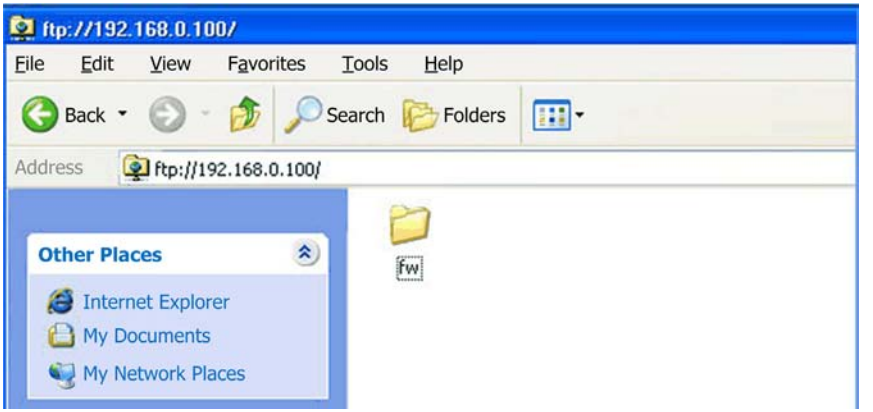
Locate the Current Firmware

View the firmware folder on your module or device by connecting with FTP:

Step	Action	Comment
1	Open Windows Explorer.	Right-click: **Start** → **Explore**
2	In the address bar, enter the Internet address for your module or device.	Use this format: `ftp://192.168.0.100/`
3	Press **Go** or **Enter**.	The browser goes to the indicated Internet address.

Step	Action	Comment
4	At the prompt, enter the user name and password.	• **User name:** pcfactory • **Password:** pcfactory
5	Press the **Log On** button.	A new window opens.

You can now see the **fw** (firmware) folder associated with your module or device:



Overwrite the Firmware

Replace the contents of the **fw** (firmware) folder:

Step	Action
1	Find the newly downloaded firmware on your local drive.
2	Open the **fw** folder associated with your device or module.
3	Replace the contents of the **fw** folder with the newly downloaded firmware files.

Power Cycle

Cycle the power to your module or device to complete the firmware upgrade and run the new firmware.

SoHVAC Data Types

D

Overview

This appendix matches SoHVAC data types with the corresponding BACnet and Modbus objects.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
BACnet Objects	196
Modbus Objects	197

BACnet Objects

This table shows the BACnet object types and the corresponding SoHVAC data types:

SoHVAC Data Types	BACnet Object Type		
	Analog	Binary	Multi-State
CJ_ANALOG	x		
CJ_BYTE	x		IF LIM_SUP<=15
CJ_CHAR	x		
CJ_DATE	x		
CJ_TIME	x		
CJ_DATETIME	x		
CJ_DWORD	x		
CJ_LONG	x		
CJ_SHORT	x		
CJ_S_BYTE	x		
CJ_WORD	x		
CJ_BIT		x	
CJ_LED			x
CJ_BUZZ			x

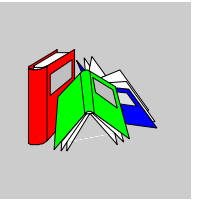
Modbus Objects

This table shows the Modbus object type for each corresponding SoHVAC data type:

SoHVAC Data Type	Modbus Mapping
CJ_BIT	1 Modbus register with a bit value in the least significant bit
CJ_BYTE	1 Modbus register with a byte value in the least significant byte
CJ_LED	1 Modbus register with LED enumeration values in the least significant byte
CJ_BUZZ	1 Modbus register with buzzer enumeration values in the least significant byte
CJ_WORD	1 Modbus register
CJ_SHORT	1 Modbus register
CJ_ANALOG	1 Modbus register
CJ_DWORD	2 Modbus registers **NOTE:** The 16 low bits are in the first Modbus register (%MW[n]) and the 16 high bits are in the second Modbus register (%MW[n=1]).
CJ_LONG	
CJ_DATE	
CJ_TIME	
CJ_DATETIME	

NOTE: Refer to the SoHVAC Software User Manual (EIO0000000537).

Glossary



A

auto negotiation

Auto negotiations allows a device at the MAC sub-layer to identify the speed (10 or 100 Mb/s) and the duplex or half mode of a connection and adjust it according to clause 28of the IEEE 802.3u standard.

B

backbone

A backbone is the main cable of a network.

BACnet

A *Building Automation and Control Network* is a communication protocol developed by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers, Inc. (ASHRAE).

BBDM

A *BACnet Broadcast Management Device* allows BACnet to manage and distribute broadcasts through IP routers. It can function in subnets that do not facilitate IP multicasting.

BIBB

BACnet Interoperability Building Blocks are function blocks that facilitate the exchange of data between devices on in a BACnet environment.

BMS

A *Building Management System* is an application of computer hardware and software that controls and monitors ventilation, lighting, power, fire-prevention, and security systems in buildings.

BootP

The *bootstrap protocol* is a TCP/IP network protocol that offers network nodes request configuration information from a BOOTP server node.

broadcast

A broadcast message that is sent out to all devices on the network.

bus

A bus is a LAN topology in which all nodes are connected to a single cable. All nodes are considered equal and receive all transmissions on the medium.

C

CoPla

These *common platform* modules facilitate plug-in communications with various protocols.

D

default

A default value is automatically assigned by the computer in a software program. Usually, this value can be changed.

device

In the broadest terms, a device is any electronic unit that can be added to a network. More specifically, it is a programmable electronic unit.

device name

The device name is a unique customer-driven logical personal identifier for an Ethernet device. a DHCP server identifies a device or module by its valid device name at power up.

DHCP

The *dynamic host configuration protocol* is a communications protocol that assigns IP addresses to devices on the network based on BootP.

E

embedded web pages

Embedded Web pages (accessed by an installed HTTP server) provide Ethernet communications modules with easy access to devices anywhere in the world from standard browsers such as Internet Explorer or Netscape Navigator.

Ethernet

Ethernet is a LAN cabling and signaling specification used to connect devices within a defined area (such as a building). Ethernet uses topology such as bus or star to connect different nodes on a network.

G

gateway

A gateway is a combination of hardware and software that interconnects networks or networking devices that are otherwise incompatible. Gateways include packet assembler/disassembler (pads) and protocol converters.

I

IEC

The *International Electrotechnical Commission* (Geneva, Switzerland) provides international electrotechnology standards.

Internet

The Internet is a series of interconnected local, regional, national and international networks, linked using TCP/IP. Internet links may be government, university and research sites. It provides E-mail, remote login and file transfer services.

IP

The *Internet Protocol* is the part of the TCP/IP protocol family that tracks the Internet addresses of nodes, routes outgoing messages, and recognizes incoming messages.

IP address

The 32-bit IP address associated with a workstation in connection with TCP/IP Internet.

L

LED

A *light emitting diode* indicates when electricity passes through it. It indicates the operation status of a communications module.

link

A link is a physical connection between two nodes in a network. It can consist of a data communication circuit or a direct channel (cable) connection.

M

MAC address

The *media access control* address of a device, which is burned into a DNI card and is added near the beginning of the packet.

Modbus

Modbus is the name of the client-server serial communications protocol developed by Modicon (now Schneider Automation, Inc.) in 1979, which has since become a standard network protocol for industrial automation.

MS/TP

The *Master-Slave/Token Passing* is used to facilitate BACnet communications over a subnetwork of BACnet translators.

N

network

A network is an interconnected system of computers that communicate and share files, data, and resources.

NTP

The *network time protocol* is a protocol in TCP used to synchronize time on devices across a network; uses signals from atomic and radio clocks.

P

PICS

The *Protocol Implementation Conformance Statement* contains the BACnet properties of a BACnet installation.

PLC

A *programmable logic controller* (or simply controller) is an industrial control computer.

port

A port is the physical connector on a device that enables an external connection.

Profibus

Profibus is an open bus system that uses an electrical network based on a shielded 2-wire line or an optical network based on a fiber-optic cable.

protocol

A protocol is a standard method of communicating over a network.

R

router

Routers can filter or forward packets based on data link layer information. Whereas a bridge or switch may read only the MAC layer addresses to filter, a router can read data such as the IP addresses and route accordingly.

routing

The routing process delivers a message across a network or networks over the most appropriate path. While simple in principle, routing uses a specialized, complex science, influenced by a plethora of factors. The more networks are joined together, the more esoteric it is set to become.

S

server

A server is a computer that provides resources to be shared on the network, such as files (file server) or terminals (terminal server).

SHI

A *Schneider host interface* is compliant with CoPla modules when a physical cavity on the host device conforms to the CoPla form factor.

SNMP

The *simple network management protocol* is a UDP/IP standard protocol that manages nodes on IP networks.

SNTP

simple network time protocol is a simplified version of NTP that synchronizes clocks in computer systems.

SoHVAC

SoHVAC for Windows is an integrated development environment for Modicon M168 programmable controllers. Those controllers let you customize and manage complex HVAC (heating, ventilation, and air conditioning) applications.

subnet

A subnet is the part of a network that shares a network address with the other parts of a network. A subnet may be physically and/or logically independent of the rest of the network. A part of an internet address called a subnet mask, which is ignored in IP routing, distinguishes the subnet.

switch

A switch is a multiport Ethernet device that increases network performance by allowing only defined communication packets on the attached individual Ethernet segments. Packets are filtered or forwarded based upon their source and destination addresses.

T

timeout

When communications stop, there may be a timeout in which the program waits the specified number of seconds before trying to communicate again

topology

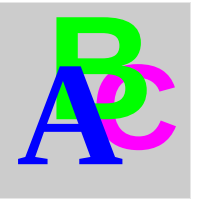
A network topology is the arrangement of the nodes and connecting hardware that comprises the network. Types include ring, bus, star and tree.

U

UDP

The *user datagram protocol* is a connectionless mode protocol in which messages are delivered in a datagram to a destination computer. The UDP protocol is typically bundled with the Internet Protocol (UPD/IP).

Index



A

agency approvals, *16*
analog value
  intrinsic reporting, *36*
Analog Value object, *31*, *89*, *144*
application, *140*, *143*

B

BACnet, *14*
  BBMDs, *164*
  broadcast, *158*
  command priority, *159*
  communications, *50*
  device identifier, *151*
  device profiles, *152*
  devices, *151*
  diagnostics, *167*
  gateways, *163*
  intrinsic reporting, *36*
  MS/TP, *54*
  object identifier, *154*
  objects, *29*, *153*
  PICS, *161*
  priority array, *160*
  properties, *155*
  property identifier, *155*
  protocol, *148*, *150*
  Protocol Implementation Conformance Statement, *161*
  routers, *163*
  services, *27*, *156*
  troubleshooting, *166*
BACnet Interoperability Building Blocks, *157*
BACnet MS/TP
  configuring, *69*
  network, *51*
BACnet/IP
  network, *52*
BIBBs, *157*
BIBBS, *27*
binary value
  intrinsic reporting, *36*
Binary Value object, *32*, *88*, *143*

C

commissioning, *67*
  SoHVAC, *74*
communication port, *17*
communications
  BACnet, *50*
configuring
  BACnet MS/TP, *69*
controller connector
  TM168BACS, *15*

D

daisy chain, *59*
Device object, *29*

diagnostics, *120*
BACnet, *167*

E

exporting
variables, *85*, *87*

F

firmware upgrade, *192*

G

grounding, *57*

I

installation, *45*
intrinsic reporting
analog value, *36*
BACnet, *36*
binary value, *36*
multi-state value, *36*

L

label
TM168BACS, *46*
TM168MODW, *46*
LED, *18*

M

mating connector
TM168BACS, *46*, *46*
TM168BACW, *46*, *46*
TM168MODW, *46*, *46*
Modbus, *14*
mounting
TM168BACS, *46*
TM168MODW, *46*
Multi-State object, *33*
multi-state value
intrinsic reporting, *36*
Multi-State Value object, *90*

N

network
BACnet MS/TP, *51*
BACnet/IP, *52*
connection, *46*
network interface connector
TM168BACS, *17*
TM168BACW, *19*, *22*

O

objects
BACnet, *29*

P

PICS, *29*
protective ground (PE), *57*
protocol
BACnet, *14*
Modbus, *14*

R

reboot, *112*
removing
TM168BACS, *47*
repeater, *54*
RS-485
cable specifications, *54*
shielding, *57*
termination, *56*

S

scanner
services, *27*
services
BACnet, *27*
scanner, *27*
shielding, *57*, *57*

SNMP, *119*
    configuring agent, *110*
SoHVAC
    commissioning, *74*
statistics, *117*, *118*, *119*

T

TCP/IP, *117*, *118*
terminator resistor, *56*
topology
    daisy chain, *59*
troubleshooting
    BACnet, *166*

V

variables
    exporting, *85*, *87*

W

web pages
    BACnet object IDs, *122*
    diagnostic log, *120*
    Ethernet TCP/IP statistics, *117*, *118*
    password, *105*
    reboot, *112*
    SNMP agent configuration, *110*
    SNMP statistics, *119*